Vol. 1 • 2021

GOOD PRACTICES IN COUNTER TERRORISM

COE-DAT
Centre of Excellence Defence Against Terrorism

Vol. 1 • 2021

GOOD PRACTICES IN COUNTER TERRORISM

Edited by Haldun Yalçınkaya

COE-DAT
Centre of Excellence Defence Against Terrorism

GOOD PRACTICES IN COUNTER TERRORISM

Yalçınkaya, Haldun (ed.) 2021
Good Practices in Counterterrorism/by Haldun Yalçınkaya (ed.)

Authors: Afzal Ashraf, Prof. Ronald Bearse, Salih Bıçakçı, Stephanie Foggett, Stephen Harley, Fulya Hisarlıoğlu, Mustafa Kibaroğlu, Susan Sim, Zeynep Sütalan, Haldun Yalçınkaya.

First Edition, Ankara, June 2021
Published by
Centre of Excellence Defence Against Terrorism (COE-DAT)
Publisher Certificate Number : 51450

Address : Devlet Mahallesi İnönü Bulvarı Kirazlıdere Caddesi No:65 Çankaya 06582
Ankara - TURKEY
P.O. Box Address : P.K.-57 06582
Bakanlıklar-ANKARA TURKEY
PHONE : +90 312 425 82 15
FAX : +90 312 425 64 89
E-MAIL : info@coedat.nato.int

Printed by Başkent Klişe Matbaacılık
Bayındır 2. Sk. No: 30/1 06420 Çankaya/Ankara (0312) 431 54 90

Disclaimer
This book is a product of the Centre of Excellence Defence Against Terrorism(COE-DAT), but does not represent the views or policies of NATO or COE-DAT. The opinions presented in the articles belong to the authors.
Includes bibliographical references and index.
Cataloguing in Publication data

152 pages;
ISBN: 978-605-74376-0-0
1. Terrorism 2. Terrorism–Prevention. 3. National Security 4. International Relations
HV6431. G663 2021 363.325 – dc23

To cite this book: Yalcinkaya, Haldun (ed.) (2021), Good Practices in Counterterrorism, (Ankara: Centre of Excellence Defence Against Terrorism)

Preface

This project began in early 2019 in my mind's eye as the Center was conducting a series of mobile education team courses and workshops on terrorism and counter-terrorism in the Middle East and North Africa regions. What was beginning to become clear for me and other COE-DAT personnel was that not only did our partners desire information to understand the terrorist threat and where it comes from; but also a deep yearning for practical solutions to the policy problems they face.

For me it all came together as I was listening to a presenter discussing the role of the military in relation to other instruments of government during one of our mobile education teams; what the Allies, partners, and other nations want is ideas of what can be done in practical means to counter-terrorism. I reflected in that moment my own journey many years earlier as I was preparing to be a military advisor in counter-insurgency/counter-terrorism where I was being provided the history, who, and what, but not the "how to" with practical solutions. During my preparation, I focused on the anecdotes, stories, and lessons learned from advisors that went before me to fill my "toolbox" with potential solutions for future unknown problems. The realization in that moment was governments and policy makers are seeking the same type of practical examples as a point to start from as they develop bespoke solutions to local circumstances.

The aim of the project is to collect "good practices" to counter terrorism that have worked in specific places and contexts that are short, but long enough to have sufficient detail, while remaining easily digestible for policy makers to serve as a starting point for their own counter-terrorism efforts. COE-DAT fully recognizes that the practices described in this book will not work in all environments as terrorism changes based of location and circumstances. However, the practices described serve to inspire thought and creativity to modify and try new approaches and ideas in the fight against terrorism.

COE-DAT recognizes that counter-terrorism is an extremely broad security challenge. COE-DAT also recognizes that military forces alone will not be able to defeat terrorism, nor should military forces be the lead agency in the fight against terrorism. Terrorism evolves from local grievances and as such requires a whole of government / whole of society approach that includes strategic cooperation and the collective action of nations, civil society, and the international community.

COE-DAT, in cooperation with academia, collects good practices in counter-terrorism and offers this publication to the NATO community, partner nations, other nations of interest, and academia in order to promulgate "good practices" in the global fight against terrorism. COE-DAT considers this book as a "living" document and will update and add more "good practices" in the coming years that combines conceptual and operational aspects of counter-terrorism.

A little about COE-DAT

COE-DAT provides key decision-makers with a comprehensive understanding to terrorism and CT challenges, in order to transform NATO and Nations of interest to meet future security challenges. This transformation is embedded into NATO's three declared core tasks of Collective Defence, Crisis Management, and Cooperative security.

As a strategic level think tank for the development of NATO DAT activities sitting outside the NATO Command Structure, COE-DAT supports NATO's Long-Term Military Transformation by anticipating and preparing for the ambiguous, complex, and rapidly changing future security environment. COE-DAT is able to interact with universities, think tanks, researchers, international organizations, and global partners with academic freedom to provide critical thought on the inherently sensitive topic of CT. COE-DAT strives to increase information sharing within NATO and with NATO's partners to ensure the retention and application of acquired experience and knowledge.

DANIEL W. STONE, Col, USAF
Deputy Director COE-DAT
May 2021

Acknowledgements

This research project would not be possible without the efforts of the authors; support team from TOBB University of Economics and Technology, as well as my staff at the Centre of Excellence Defence Against Terrorism.

I want to thank the authors Stephen Harley, Susan Sim, Salih Bıçakçı, Ronald Bearse, Mustafa Kibaroğlu, Afzal Ashraf, Stephanie Foggett, and Zeynep Sütalan for their valuable academic knowledge and insights into practical solutions to counter-terrorism that made this book a reality. I especially want to thank Stephen Harley and Afzal Ashraf who through no fault of their own were the inspiration for the development of this book.

COE-DAT is grateful to our academic assistants Alice Lõhmus and Elif Merve Dumankaya, our assistant project manager Fulya Hisarlıoğu and particularly our lead project manager Prof Haldun Yalçınkaya (Chair of the Department of Political Science and International Relations at TOBB University of Economics and Technology) for assisting COE-DAT to conceptualize and organize the book project.

I am highly indebted to members of my staff Col (ret) Mustafa Özgür Tüten (previous director), Col Daniel W. Stone, Col (ret) Mustafa Doğan, Col Pavlin Raynov, Col Kadir Özyurek, Col Attila Csurgo, Col Ioan Pribek, Maj Ian McDonald, Maj Michael Pasquale, Maj Zekeriya Tosun, Maj Bert Venema, and Capt Gökhan Cin for their endless patience, tireless work, critical reviews, and passion to complete this book. A special thanks goes to Ms Selvi Kahraman because without her computer skills we could never have been able to coordinate this project with our team members all around the world.

Barbaros DAĞLI
Colonel (TUR A)
Director COE-DAT

TABLE OF CONTENTS

CONTRIBUTORS (*in the order of alphabet)*

Dr. Afzal Ashraf is an Assistant Professor of International Relations and Security at the University of Nottingham. He has served in the UK Armed Forces as a senior officer and has experience of diplomacy within the UK's Foreign and Commonwealth Office as well as of counter terrorism policy and operations within various UK departments. He has also worked at a security Think Tank and has been an Academic Advisor to NATO's Centre of Excellence for Defence Against Terrorism.

Prof. Ronald Bearse has been helping organizations manage risk and protect critical infrastructure in an increasingly complex and challenging threat environment for 30 years. He has served in a wide variety of analytical, operational, managerial and senior leadership positions with the U.S. Departments of Defense (DOD), Homeland Security (DHS) and the Treasury (TREA), including positions as: Chairman, US National Security Council's Asset Protection Working Group where he was instrumental in broadening the US Key Asset Protection Program; TREA Liaison to the US Critical Infrastructure Assurance Office, Director, Office of Security and Critical Infrastructure Protection; TREA's first Critical Infrastructure Protection Officer; and Director, Business Continuity and Emergency Preparedness Staff, DHS National Protection Programs Directorate (now the US Cybersecurity and Infrastructure Security Agency). Academically, he has served as: Senior Fellow, George Mason University's Center for Critical structure & Homeland Security; Academic Advisor/ Lecturer, NATO, Center of Excellence Defense Against Terrorism (COE-DAT) on critical infrastructure protection against terrorist attacks; and Adjunct Professor in the Emergency Management and Homeland Security Program at the Massachusetts Maritime Academy. Ron has an MPA from George Washington University and is a Distinguished Graduate of the US National Defense University.

Prof. Salih Bicakci is the Professor of International Relations at Kadir Has University, Istanbul. He completed his B.A. on History at Marmara University Education Faculty in 1994, and his M.A. at Marmara University Turkic Research Institute in 1996. Bicakci received his PhD from Tel Aviv University in Israel in 2004. Prof. Bicakci began his academic career at Işık University and took part in numerous academic projects on identity, security and terrorism. He has thought classes in several national and international universities on the Middle East in International Politics, International Security, International Relations Theory and Turkish Foreign Policy. He has made evaluations and presentations on cyber security at the NATO Defense Against Terrorism Centre of Excellence (COEDAT), NATO Command and Control Centre of Excellence (C2COE) and NATO Maritime Security Centre of Excellence. He has though Cyber Security and Middle Eastern Security courses at the Armed Forces Academy of the Turkish War College. He has presented on international security and cyber security in several international academic conferences.

Stephanie Foggett is a Resident Fellow at The Soufan Center and the Director of Global Communications at The Soufan Group. She leads on strengthening engagement with media and strategic partners on matters relating to international security and counterterrorism, including a focus on terrorism and extremism online and in the information space.

Stephan Harley is a former British Army officer who has latterly worked in Iraq & the pan- Arab region for the US government, in Afghanistan for NATO and in Somalia for the UN and the UK Foreign and Commonwealth Office in the fields of counter-terrorism, Preventing & Countering Violent Extremism (P/CVE) and Strategic Communications. He currently works for the British Embassy Mogadishu with a broad remit of building confidence in the Federal Government of Somalia and countering the al-Qaida linked terror group, al-Shabaab. He has published extensively on Somalia, most recently contributing two articles to the UN's seminal study, 'War and Peace in Somalia: National Grievances, Local Conflicts & al-Shabaab', as well as covering East African issues for The Economist Group. He can be contacted at stephenharley@me.com

Dr. Fulya Hisarlioglu has a PhD in Political Science. She conducted her PhD on Turkish Foreign Policy with a special focus on Cyprus Conflict. She specialized in Turkish Foreign Policy, critical geopolitics and critical security studies. She delivered lectures in various universities on European security, diplomatic history and comparative political systems. Hisarlioglu took active part in several projects organized in collaboration with NATO Public Diplomacy Department and Turkey's Council of International Relations Association. She published various book chapters, opinion papers and journal articles in the Social Science Citation Index journals such as Geopolitics and International Relations. She continues her academic carrier as the part-time lecturer in Kadir Has University.

Prof. Mustafa Kibaroglu conducted his PhD at Bilkent University International Relations Department. He is currently the Dean of the Faculty of Economics, Administrative and Social Sciences and the Director of the Center for International Security Studies and Strategic Research (MEF_Strategy) at MEF University in Istanbul. He used to teach courses on "Arms Control & Disarmament" and "Turkish Foreign Policy" in the Department of International Relations at Bilkent University in Ankara from 1997 to 2011 where he was also the Vice-Chair of the Department. Prof. Kibaroğlu was a Research Fellow at the United Nations Institute for Disarmament Research in Geneva (1995); International Atomic Energy Agency Fellow at the University of Southampton (1996); Post-doctoral Fellow at the Monterey Institute in California (1996/97); and Sabbatical Fellow at the Belfer Center of Harvard University (2004/05). Prof. Kibaroğlu is the co-author of Global Security Watch – Turkey (2009) by Praegers in the United States, and the co-editor of Defence Against Weapons of Mass Destruction Terrorism (2010), Bioterrorism: Threats and Deterrents (2010), Responses to Nuclear and Radiological Terrorism (2011), Defence Against Terrorism (2011), and Analysis and Strategies to Counter the Terrorism Threat (2011) by IOS Press in Netherlands. He is also

the author and co-author of numerous chapters in books and articles in academic journals, such as Security Dialogue, Nonproliferation Review, Bulletin of the Atomic Scientists, Middle East Quarterly, Middle East Journal, Brown Journal of World Affairs, Middle Eastern Studies, Korean Journal of Defense Analysis, Turkish Studies, Middle East Policy, and Journal of Balkan and Near Eastern Studies. Prof. Kibaroglu used to be the Academic Advisor of the NATO Centre of Excellence Defence Against Terrorism (COE-DAT) between January 2006 and January 2013. In the meantime he was the Editor-in-Chief of Defence Against Terrorism Review (DATR) published by COE- DAT.

Susan Sim has worked in various capacities in the Singapore government—in law enforcement, intelligence analysis, and diplomacy—and was a journalist based in Indonesia in the 1990s. A graduate of the University of Oxford, she started her career in Singaporean government as a probationary police inspector. In 2009, she founded Strategic Nexus Consultancy, a boutique research firm specializing in home-front security and counter-terrorism issues, in which capacity she led several commissioned research projects studying the terrorist landscape and government responses in Southeast Asia. In December 2010 she joined The Soufan Group, combining her local knowledge with the expertise of TSG's international team. She has three books published by prestigious press agencies and she contributed several studies in edited books. Her most recent book, The Ostrich, the Ah Long, the Con Woman and the Creepy Guy: The Story of Crime Prevention in Singapore (co-written with chief police psychologist Majeed Khader), was launched in July 2017 by Home Affairs Minister K. Shanmugam. She was on the board of the National Crime Prevention Council of Singapore for nine years and in 2018 was awarded the Public Service Medal (National Day Awards) by the President of Singapore.

Dr. Zeynep Sutalan holds a PhD degree in International Relations from the Middle East Technical University. Between the years 2005 and 2011, she worked for the Centre of Excellence Defence Against Terrorism (COE-DAT) as a concept specialist. She has been giving lectures about terrorism in COE-DAT and Partnership for Peace Training Center in Ankara. Her academic interest includes terrorism, counterterrorism, gender and terrorism, history, politics and economics of the Middle East. Currently, she is a part-time lecturer at the Atılım University.

Prof. Haldun Yalcinkaya is an International Relations Professor in TOBB ETU University. Prof. Yalcinkaya graduated from Kuleli Military High School and later Turkish Military Academy. During his military service as an officer, he completed his post-graduate studies in International Relations at İstanbul University. After earning his PhD degree, he conducted postdoctoral studies at Oxford University, West Point Military Academy and the University of Florida. He published two books on war issues and several academic articles. After serving more than ten years at Turkish Military Academy, he has been Associate Professor in International Relations at TOBB University of Economics and Technology since 2013.

INTRODUCTION

Haldun Yalcinkaya

GOOD PRACTICES IN COUNTERTERRORISM

Humanity is currently facing one of the most asymmetrical, constantly evolving, and intimidating human-made threats; terrorism. It is clear that today's terrorist networks are aware of the technological and social benefits our times offer which, unfortunately, enables increasingly sophisticated transnational terror networks. In the hands of present-day terrorists, any component of daily life (commercial airplanes, physical and cyber systems controlling critical infrastructure, social media platforms, cryptocurrencies, even the laboratories in our hospitals) can be innovatively utilized to cause mass destruction, to finance terrorist activities, to reach out to a wider audience, to recruit new sympathizers, or to damage social cohesion. Acknowledging the endless possible attack scenarios posed by the new generation of terrorist networks and considering the vulnerabilities of our highly integrated societies, there is no alternative but to evolve counterterrorism (CT) policies in a unified manner.

This book is a policy-analytic collection, which came about from the commitment of highly respected researchers and practitioners. In an effort to provide answers and potential responses to the aforementioned agenda of current CT policies and practices, NATO Centre of Excellence for the Defence Against Terrorism (COE-DAT) initiated a "Good Practices in Counterterrorism" handbook project with the academic support of TOBB University of Economics and Technology. The book aims to present successful strategies and policy alternatives in the field of CT by examining various cases. This timely contribution offers a comprehensive and multi-sectoral approach to support efforts in the CT domain through inspiring various actors in their ongoing endeavors to develop, professionalize and synchronize various CT policies at the national level. This book is the final outcome of a one- year endeavor, that started in early 2020 and which has built an interactive platform of expertise on the effective methods, strategies, national responses, and alternative models in CT.

Although the project was initiated after one year of preparatory work, it is built upon the accumulation of COE-DAT and project contributors' competences and depth of understanding. Undoubtedly, the chapters in this book are not the only expertise COE DAT has accumulated so far. It is only the first package and later the center will keep sharing the knowledge, accumulated over the years, on good practices in CT. This is to say; the readers should know this book is just the first volume. As a strategic level think tank, working for the development of NATO-Defence Against Terrorism activities, COE-DAT supports NATO's Long-Term Military Transformation by anticipating and preparing for the ambiguous, complex, and rapidly changing future security environment. Sitting outside the NATO Command Structure, COE-DAT interacts with universities, think tanks, researchers, international organizations

and global partners with the academic freedom to provide critical thought on the inherently sensitive topic of CT. The Centre strives to increase information sharing within NATO and with NATO's partners to ensure the retention and application of acquired experience and knowledge. It supports NATO allies, Sponsoring Nations, NATO Partners, non-NATO entities, and other stakeholders in their CT efforts with emphasis on military effectiveness and interoperability amongst assets, forces, and capabilities. In order to contribute to the standardization and professionalization of CT practices, the organization delivers regular meetings, courses, seminars, workshops, lessons learned evaluations and analysis, academic research programs and projects, as well as publishing extensively on the subject of CT.

Against this background, COE-DAT provides a sophisticated intellectual platform enabling CT stakeholders (military officials, policy makers, academics, CT experts and so on) to draw lessons from CT field-tested practices and share profound information on policy alternatives and possible future threats driven by the national and case specific experiences in this dynamic and complex domain. In line with this, the "Good Practices in Counterterrorism" collection is the latest initiative that aims to fill the gap in CT literature and policy-making through presenting field-tested and evidence-based good practices as well as innovative models addressing current trends and future threats in CT. This book will contribute to the global CT agenda that involves the harmonization of CT requirements, pooling and sharing expertise in the field, setting priorities, standardizing CT mechanisms, and facing new security challenges. In the meantime, this publication will support policy-makers and high- level practitioners to transform their CT framework based on the alternative solutions to deal with relevant aspects of CT practices.

Structure of the Book

Developing a book that covers all aspects of CT is an extremely ambitious task. However, the ultimate intention of the project is to keep this book series updated and under constant review, enriching the content through adding new good practices covering emerging debates in CT. Therefore, the book is intended to be a living document that will be enriched and improved in time through additional volumes. The topics covered in this first volume are limited and dictated by the extent to which they seek practical solutions for a group of select challenges in the field of CT. The collection of good practices presented in this book is the first step. This publication is not recommending any action that is incompatible with national laws and regulations. Having this reality in mind, the lessons identified are generic, flexible, and adaptive rather than binding, prescriptive, and rigidly precise. We also underline the fact that chapters are penned based upon open-source information and unclassified documents produced by national authorities and regional and/or international organizations.

The first chapter, which elaborates upon the conceptual framework, is dedicated to discussing the counterterrorism puzzle and evaluating the ways this study integrates evaluative research as a policy analytic framework into the field of CT. Fulya Hisarlıoğlu and Haldun

Yalçınkaya underline the centrality of achieving an agreed upon definition of terrorism in order to enable strategic cooperation and effectively manage national and international CT policies. While the authors highlight the context-dependent nature of CT policies, they argue that extension of the CT repertoire can only be achieved through the constant exchange of "know-how" and CT experiences, which may uniquely enlighten us about the commonalities but also the differences within terrorist activities and CT responses. Adopting the strategy of "learning from each other", lessons drawn by good practices and capability assessments built on maturity models are at a premium. Based on this, they point out that in order to contribute to the professionalization and standardization of CT policies, the most efficient way forward is to discuss and document good practices, effective implementations and capacity building maturity models which reflect cutting-edge expertise and/or experience.

In the second chapter, Stephen Harley considers good practice in the use of soft-power, hard- power, and smart-power tools. He discusses how soft power and public diplomacy can be utilized to prevent international support for terrorist networks and to create a multilateral platform to cope with terrorism. The isolation of terrorist groups through diplomacy and soft power mechanisms contributes to the military battle against terrorism. This chapter explores the existing doctrinal definitions of hard and soft power in parallel to CT and counter- insurgency. At the same time, it questions whether the soft/smart power focus in this realm is primarily focused on Preventing & Countering Violent Extremism (P/CVE) and its antecedents such de-radicalisation/counter-radicalisation. A direct correlation between hard power and counterterrorism or soft power and P/CVE is not taken for granted, but provides a useful initial structure for the discussion. The various activities across the spectrum of hard and soft power (military, policing, intelligence, legal, economic, diplomatic, informational, educational, developmental) are defined and explored using brief case studies on Norway, Denmark and Turkey, and a longer study focused on Somalia. The chapter concludes by reviewing the challenges inherent in the way hard and soft power are currently perceived, and how these challenges might be overcome to achieve "smart power", the combination of hard and soft power.

In the third chapter, Susan Sim, in her study on the national capacity building efforts, introduces Singaporean and European Union authorities' counterterrorism programs and strategies. . Policy guidelines and strategy papers, drawn from practices at the national level, highlight the operational, political, and societal dimensions of a dynamic and well-orchestrated CT structure. Although most states have published their national CT strategies, very few have published detailed national action plans. The EU's peer evaluations of member states' anti-terrorism arrangements, declassified in most parts several years after they were first composed between 2003 and 2005, is one of the few sources of effective practices in the implementation of national CT policies, especially as those practices were then shared with other states with little historical experience in handling domestic terrorism. It focused on the national responsibilities at government ministry, security and intelligence service and law enforcement agency level; offered as recommendations closing security gaps and enhancing existing capacities from an operational and practical perspective, with each state free to implement them according to its national legal and political framework. Although adaptable and robust national security policies should be able to pivot to deal with new challenges, the long-term terrorist threat is challenging to institutional and societal resilience, as many countries have

come to realize. The theme for year 2020's UN High-level Conference on Counterterrorism was "Building Institutional and Social Resilience to Terrorism". This chapter also examines how a small city-state like Singapore has been building a national counterterrorism program "to sensitize, train and mobilize the community to play a part to prevent and deal with a terrorist attack". Called SG Secure, it is hinged around convincing people that every individual must assume some self- responsibility for protection against risk, for good relations between communities, and that everyone, including the private sector, must do its part to shore up societal and national resilience. Her analysis of the success of SG Security program illustrates that Singapore might be considered as one of the best cases in which the military sector raises popular awareness and the integration of society into the larger framework of CT.

The fourth chapter of this book is dedicated to a discussion of cyber security in CT. Professor Bıçakçı introduces his own maturity model that elaborates on capacity building and risk management in cyber security in the domain of CT. The author questions the ways that have been promoted to protect cyber domains from terrorist attacks. The chapter addresses the necessity of the detection and elimination of vulnerabilities of a sector or country specific computer systems (hardware, software, data-connection layers like fiber optics, land lines etc.) to minimize cyber-attack risks. Through developing a model called the Cyber Security Maturity Model, the chapter introduces a holistic approach in which both technical (computer systems) and behavioral (human factor and decision-making process) vulnerabilities are revealed and the whole system is re-organized in order to manage risks in the domain of cyber security. The research discusses the five steps of the Cyber Security Maturity Model, which would strengthen computer system structures against an attack. The first step addresses basic security precautions in computer systems and a lack of regulation regarding to cyber security both in level of policy and division of labor. The second step is called "Developing", and includes the introduction of principle security procedures in the layers of human, technology, and infrastructure. The Cyber Security Maturity Model improves all these layers with three additional steps. The next step defines a baseline of required security settings. The model then continues with Managed and Optimized levels which form a robust system to defend cyberspace from major types of cyber- attacks.

In the next chapter, Ronald Bearse discusses CT policies in the framework of Critical Infrastructure Protection (CIP). The survival and sustainability of society is dependent on the protection of daily life support systems, known as critical infrastructure. Our heavy dependence on complex and intertwined infrastructures requires further vigilance and resilience. Apart from physical-material structures, life support systems are becoming more dependent on information and communication technologies. The connection of the physical world and cyberspace necessitates a multi-sectoral and multilateral approach to address the protection of critical infrastructure in the context of international terrorism. Although critical infrastructure protection is mainly viewed as being a national practice, risks and threats posed by terrorist activities targeting national infrastructures can best be detected and managed through effective intelligence sharing, public-private sector cooperation, and international resilience in this field. In order to address these vulnerabilities and to discuss possible solutions, this chapter aims to shed light on national good practices in the domain of CIP and how they can be utilized by NATO and Partner Nations to strengthen their national security, national economic security, and national public health and safety postures in an increasingly challenging international security environment. It also discusses the nexus between CIP, Critical Infrastructure Security & Resilience (CISR) and counterterrorism and provides government

and private sector senior officials with a forward-looking plan of action for building, implementing, and maintaining demonstrable CISR capacities and capabilities.

Another critical CT field covered in this study is the countering of Weapons of Mass Destruction (WMD) terrorism. Having the potential to inflict catastrophic damage on the target, WMD best serve terrorist groups that are fanatically irrational with regard to causing mass casualties. Acknowledging the high destructive power of WMD, enhancing preparedness against the potential security risks posed by the possession and use of WMD by terrorist groups and radicalized individuals requires multilateral action and far-reaching cooperation. This chapter is designed to present good practices, which enable national actors countering WMD terrorism through specific strategies such as the effective detection of terrorist groups' access to WMD supplies and equipment; deterring support for WMD terrorism; enhancing resilience and preparedness against WMD terrorism, and active intelligence sharing. Mustafa Kibaroğlu introduces a group of international efforts and good practice examples on monitoring the trafficking and possession of nuclear WMD. The Cooperative Threat Reduction (CTR) Program, also known as the "Nunn-Lugar Program", is presented as a tangible international effort that aimed to assist the former Soviet republics to destroy weapons of mass destruction and their associated infrastructure in order to reduce the chances of the material used in their manufacture falling into the hands of terrorist groups or some states of concern. Nunn-Lugar has been one particular domain of intensive cooperation and collaboration between the United States and Russia that has not been negatively affected by the deterioration of relations between the two states in the post-Cold War era. In the same vein, Professor Kibaroğlu introduces the IAEA's Nuclear Security Guidelines (INFCIRC/225) and IAEA's Illicit Trafficking Database Program (ITDP), as the fundamental positive steps in international community's endeavors to eliminate terrorist groups' possession and use of WMD. Although not mandatory, these practices are adopted by most states and have been made a requirement through bilateral agreements. Involving the voluntary notification by government authorities of illicit trafficking incidents, ITDP provides a valuable source of information that helps the member states to better understand threats and vulnerabilities.

Afzal Ashraf and Stephanie Foggett continue with their analyses of the use of conventional and social media by terrorist networks for a variety of purposes and elaborates on the national practices in dealing with these malicious activities. The chapter begins by looking at the utility and importance of communication to terrorists and in so doing makes a distinction between the message and the medium using a historical approach to show continuities and discontinuities in both the message and the means used to spread it. It focuses on online communications but also covers 'mass communication' more generally, to evaluate how terrorists take advantage of contemporary channels including TV, radio, and the traditional news media. The relationship between conventional mass communications and online communications, especially social media, is explored to define the increasingly interdependent nature of these two mediums. The same approach is applied to the efforts by CT organizations to respond to terrorist messaging, especially after its emergence online. The purpose is to develop an understanding of the principles, which rarely change, and of the practice, which is continually evolving. That way the relevance of the work can largely transcend any practices and examples that it may be based upon. The simultaneously and multiple use of communication mediums for activities such as propaganda, intelligence gathering, surveillance, recruitment, fund raising and so on is also explored. The challenges and opportunities

for analysis of these highly complex and nuanced forms of communications is discussed, particularly aspects dealing with the use of language, network analysis, artificial intelligence, and big data. This discussion is bounded by the impact of wider issues such as legal, social, and privacy constraints. The impact of these constraints both in monitoring the terrorists' use of the internet and in responses to it, especially in the form of counter narratives and counter radicalization activities to protect especially vulnerable groups, is explored with a view to identifying responses that are both acceptable and effective.

Zeynep Sütalan discusses the gender aspect of successful CT policies in the last chapter. Women are generally perceived as the victims of terrorism. However, this is only a partial understanding of women's role in terrorism and counter terrorism. Some women are at the same time voluntary participants of violent extremist movements and terrorist activities. Increasing numbers of women Foreign Terrorist Fighters in ISIS is one of the most significant instances underlining women's agency in terrorism. Acknowledging and freshly questioning the agential power of women in both terrorism and counter-terrorism enables us to better address the terrorist threat and develop efficient CT programming. In the light of case studies and conceptual explanations, this article examines the gender aspect of, but primarily the role of women in, CT and Countering Violent Extremism (CVE) over the apparent "success stories" in order to obtain good practices which can be applied to similar contexts. Though not immune from deficiencies, there are certain practices that can be identified as good practices in the gendered delivery of CT and CVE. Therefore, in regard to the success stories in addressing the gender aspect of counterterrorism, this chapter utilizes three case studies: mother schools, Female Engagement Teams (FETs), and Gender Advisors (GENADs) to highlight the different roles women can play with regard to CT. These case studies, of just three of the roles women can play in CT and CVE as preventers, counterterrorists, and change-makers, are scrutinized in relation to three different levels of analysis, the local, the operational and the cultural- institutional levels. Apart from being widely referred to as successful examples of CVE and CT programming, these initiatives are not immune from criticism. One of the most important arguments revolves around the measurement of success. How do we measure success in CVE and CT programs? The author concludes that apart from the FETs, the success of which are assessed due to their 'operational effectiveness', the more we move to the area of CVE, the less we will be able measure success due to the lack of scientific tools.

CHAPTER I

CONCEPTUAL FRAMEWORK: COUNTERTERRORISM AND GOOD PRACTICES

Fulya Hisarlioglu

Haldun Yalcinkaya

Soon after the 9/11 the "war on terrorism" became the number one agenda item in international fora. However, war and terrorism are philosophically two different concepts which need to be discussed separately. In fact, some war scholars highlighted their objection to the doctrine of the "war on terrorism" due to the fact that this was philosophically an oxymoron. On the one hand, as Carl von Clausewitz stated in his seminal work, On War, war is a duello which occurs between two parties. In duello, warring parties might be at times the attacker and at other times the victim. On the other hand, terrorism is a triello, which means there are three parties involved in terrorism. The first party is the attacker, the terrorist, and the second party is the victim of terrorism. But the first and second parties act on a stage in front of bystanders. The bystanders are equally the target of the action taking place on the stage. The action on the stage results in a fear among the bystanders through seeing, hearing or learning of the attack. But, in fact, the victim is not a target at all: the target does not necessarily have to be hit by, say, a bullet. Instead the target is the third party who is effected through intimidation. This approach to understanding terrorism demonstrates the philosophical approach inherent to terrorism and establishes a basis for the subsequent conceptual explanations for terrorism, as well as for counterterrorism.

This chapter, addressing the contested nature of terrorism and counterterrorism, starts its analyses with the conceptual and operational challenges that hinder national and international actors in effectively coordinating counterterrorism (CT) policies. The second part of the chapter aims to build a bridge between CT domain and quality management studies which can be utilized strategically by CT policy-makers and civilian and military CT professionals. We argue that one of the most dramatic challenges is the conceptualization puzzle that fragments the CT community at both the strategic and operational levels. On the other hand, the September 11, 2001 tragedy triggered a new process in which CT policy-makers and international security actors achieved common ground about the urgent necessity to professionalize and standardize CT policies. Starting from the early 2000s, drawing lessons from other countries' success stories and good practices inspired policy transfer experiences which became important assets in handling terrorism.

Conceptual and Operational Evolution of Terrorism and Counterterrorism

Agreeing on a universally agreed definition of terrorism is becoming much harder but is also more essential than ever, due to the fact that it determines the success of CT policies and facilitates strategic international cooperation.[1] Yet the ongoing conceptual conundrum fragments the literature and creates inconsistencies in practical and tactical terms.[2] As Richardson notes, "the failure to craft an agreed definition of terrorism has left a vacuum for actors, whether they be state or non-state, to define terrorism in ways that serve their own perceived political and strategic interests, and, in the case of state responses, remits of 'counterterrorism' are often determined accordingly".[3] Moreover, lacking an agreed definition, the term terrorism is widely and carelessly used in many contexts in such a way as to almost undermine the brutality of terrorist activities.[4] In the domain of CT, the golden principle, therefore, should be developing a comprehensive definition of terrorism in order to eliminate counter-productive policies and encourage a comprehensive campaign for countering terrorism.

Dictated by the September 11, 2001 tragedy, the necessity of a comprehensive approach in defining terrorism was reiterated.[5] One of those seminal contributions was introduced by Hoffman who defined terrorism as the "deliberate creation and exploitation of fear through violence or threatened violence in the pursuit of political change. Terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or object of the terrorist attack. It is meant to instill fear within, and thereby intimidate, a wider 'target audience'".[6] Although the debates on the conceptualization of terrorism continues at the academic, political, and practitioner levels, the international community too, under auspices of the United Nations (UN), could barely achieve a non-binding definition of terrorism. The UN definition of terrorism introduced a broader framework in which diverging means, motivations and activities of terrorists were underlined. In the UN's Security Council Resolution 1566 (2004), the UN urged its member states to identity any activities as the manifest practices of terrorism as:

> Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial,

1 Martini and Njoku, *The Challenges of Defining Terrorism*, 75.
2 Davis and Cragin (eds), *Social Science for Counterterrorism*, 3-5.
3 Richards, *Conceptualizing terrorism*, 3.
4 Schmid, *The Definition of Terrorism*, 89.
5 Schuurman, Research on Terrorism, 2-5.
6 Hoffman, *Inside terrorism*, 45.

ethnic, religious or other similar nature…[7]

The resolution also called upon all member states to contribute to international efforts in countering terrorism, to prevent such acts, and to ensure them that "such acts are punished by penalties consistent with their grave nature". In the same vein, NATO developed its own conceptualization and announced that any "unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives"[8] would be counted as terrorism.

In the post 9/11 era, the bourgeoning literature on the conceptualization of new-age terrorism concentrates not only on violence and criminal strategies but also on the ideological background and motivations as well as the antagonistic nature of terrorism and the socio-political context of terroristic activities. To Nalbandov, the ideological turn in conceptualizing terrorism leaves more room for comprehensive CT policies that target not only terrorism but also its root causes.[9] In the current circumstances, there is a consensus that relative success achieved by hard power CT policies have to be supported by smart defense strategies based on political ownership, community-based policies, multi-national and multi-sectoral cooperation, and societal support. "Thus, the only way for a state to survive against terrorism is to wipe it out completely—that is, in absolute terms. The relative terms, however, is there the counterterrorism actors have serious problems in defining what is that they are striving to achieve. [*sic*]"[10] With respect to this, the CT field in both the intellectual and the operational sense is going through a fundamental re-construction in the way it targets terrorism and its root causes in every sphere of life. This enlightenment in the CT field has taken its place in multilateral arrangements. The UN adopted a CT document "with a view to adopting and implementing a strategy to promote comprehensive, coordinated and consistent responses, at the national, regional and international levels, to counter terrorism, which also takes into account the conditions conducive to the spread of terrorism".[11] In the same vein, NATO's understanding of strategic cooperation integrating civilian and military perspectives[12] has been transferred into the domain of CT. NATO adopted a sophisticated conceptualization of CT by including "all preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals and property against terrorist threats and/or acts, to respond to terrorist acts. In the frame of the NATO Comprehensive Approach, this can be combined with or followed by measures enabling recovery after terrorist acts".[13] The increasing emphasis on the elimination of vulnerabilities in the fight against terrorism underlines the urgent necessity of sharing experience and intelligence to re-calibrate

7 UN, *Security Council Resolution 1566 (2004)* 2.
8 NATO, *NATO Military Committee Concept for Counter-Terrorism*.
9 Nalbandov, *Evaluating the 'Success'*, 91-115.
10 Nalbandov, *Evaluating the 'Success,* 92.
11 UN, *The United Nations Global Counter-Terrorism Strategy*, 2.
12 For more information, please see: NATO, NATO Civil-Military Co-Operation (CIMIC) Doctrine AJP-9, June 2003.
13 NATO, *Military Committee Concept for Counter-Terrorism*.

national threat assessment structures, to enhance CT-related capacity development and to "improve resilience by strengthening national capacities for civil preparedness and homeland security".[14] In addition to this, evolution of CT policies targeting absolute success enlarges the CT framework by including the strengthening of policies to combat violent extremism and the radicalization of vulnerable social groups.[15] In the overall analysis, opening new spaces of opportunity for multi-sectoral and multilateral dialogue may be the silver bullet in the development of national and international level CT policies to overcome contemporary terrorism.

Good Practice as an Alternative Framework for Standardization

Achieving a comprehensive approach to address terrorism and to standardize CT policies is quite puzzling and difficult, predominantly due to the individual character of this policy field. CT policies are generally situated at the intersection of national and transnational jurisdiction.[16] This hinders the international community from dictating any authoritative measures or doctrine-like binding provisions on the nation states which would jeopardize the crown principle of post-Westphalian world order - the principle of modern international law predicating that each nation-state has sovereignty over its territory and domestic affairs. Acknowledging the aforementioned contested character of the policy domain, we introduce a non-binding policy guideline and a general framework that would catalyze harmonization and standardization of CT practices in line with multilateralism and strategic cooperation. Having this reality in mind, the lesson drawing attempts that follow generic, flexible, and adaptive guidelines rather than binding, prescriptive and rigidly precise measures.

Extension of the CT repertoire can only be achieved through the constant exchange of "know-how" and CT experiences that may enlighten us about the commonalities and differences among terrorist activities and CT responses. Adopting the strategy of "learning from each other", this scholarly attempt acknowledges that lessons drawn from good practices and capability assessments built on maturity models are at a premium. Based on this, we believe that, in order to contribute to this field, the best approach is to discuss and document good practices, effective implementations and/or capacity building maturity models which reflect cutting-edge expertise or experience. In order to address challenges and enable policy innovation, good practices provide evidence-based research that is "based on scientific and analytic knowledge that rigorously examines their impact on outcomes"[17] Inspired by the UN Counterterrorism Executive Directorate's evaluations, we acknowledge a good practice as "a technique, an activity, a strategy, a methodology or approach that has been shown, through application and evaluation, to be effective/and or efficient in achieving a desired result".[18]

[14] NATO Secretary General, *NATO 2030*, 32-33.
[15] For more information, please see: UN General Assembly, Plan of Action to Prevent Violent Extremism, UN General Assembly Resolution A/70/674, 24 December 2015.
[16] Bowman, *Terrorism Challenges*, 45.
[17] Lum and Kennedy, *Evidence-based Counter-terrorism*, 4.
[18] UN, *Framework for the Collection*.

In her study on evaluative counterterrorism research, De Graaf underlines the delicate domestic and international environment in which the policy practitioners have to conduct their CT campaigns.[19] Most of the time, civilian and military practitioners deal with preventive and responsive CT measures under the pressures of scarce resources (budgetary constraints), public opinion (popular-political constraints), national and international administrative constraints (limited cooperation or coordination), as well as judicial and ethical constraints.[20] In this way the effectiveness of CT policies turn into a test of legitimacy and credibility[21] for democracies. In order to deal with the burdens of CT interventions, lesson-drawing from the success stories seems to be effective in saving national resources and building a global consensus in the standardization and professionalization of CT policies. Moreover, scientifically robust evaluations also shed a light on the emerging and potential risks that will turn into destructive means in the hands of terror-affiliated groups. With this regard, evaluative researches' key principles, including in-depth and systematic analyses of the policy tools and measures; "disseminating, translating, and using research to inform practice; engaging in partnerships that foster evaluation (i.e., between practitioners and researchers); and expanding the collection of high-quality data"[22], should be transferred into the national and international CT policy making affords. Thus, from a policy analytic perspective, policies developed through scientifically robust evaluative research designs, inspired by the good practices and lesson-drawing are acknowledged as some of the most efficient performance improvement efforts in the domain of CT.

Yet the success of policy transfer is heavily dependent on a set of variables such as policy environment, human capital, organizational/institutional structure, and selection of the most appropriate 'good practice' cases. Thus the gold standard in policy transfer through policy evaluation is being inspired by the truest practices that can be appropriated.[23] Therefore it should be noted that good practices are context-dependent and they are not 'good' for everyone. In this sense, defining a case as a good practice is by itself quite a challenging occupation and it requires proficiency and experience in the policy field.

Despite the aforementioned strengths of using good practices as strategic tools to organize and standardize national and international CT policies, they might also provide some constraints. Most CT related policy areas are dynamic and change rapidly over time, and across culture and national institutional settings. For example, standardization of CT policies in the domains of cyber security and other policy sectors which are intimately affected by changes in information technologies - such as critical infrastructure security, social media, border surveillance and so on - requires further vigilance and resilience due to the hyper-dynamic character of the policy sector. In other words, what the good is today might not be the good tomorrow. The chapter on cyber security presented in this book points

[19] De Graaf, *Evaluating Counter-terrorism*, 6; Lum and Kennedy, 4-5.
[20] De Graaf, *Evaluating Counter-terrorism*, 6.
[21] Lum and Kennedy, 4-5.
[22] Ibid, 4.
[23] Lum and Kennedy, *Evidence-based,* 8.

out the wider relevance of this change process and introduces an authenticated maturity model as a risk management and resilience strategy. Secondly, CT policies are structured in complex operational environments. Any improvement or change in a single CT sector can result in dramatic consequences in other, related sectors. This necessitates a holistic approach in which all aspects of CT are included in the assessment process. Regarding the nested nature of CT operations, reliance on capacity building on the basis of a single CT sector would not guarantee the overall transformation of CT policies. This debate is explored in depth in this collection in the discussions on cyber security, critical infrastructure security and resilience, and the use of social media by terrorists and by CT practitioners. Last, but not least, all assessments based on good practices suffer from the lack of broadly accepted measurement principles, standards and methodologies. Although the number of terrorist attacks prevented by the operationalization of professional CT operations might give an indicator of how to measure success, successful CT policies also enable social, political and economic betterment: but these are more difficult to measure.

At this point, we should also assess the long-term impact of CT policies on a social, political, and economic basis. In order to address this issue, our authors employ a strategic methodology of covering success stories which reinforce national and international cooperation as well as social cohesion and resilience. Susan Sim, in her chapter on the institutionalization of CT policies, discusses in-depth the problem of the measurement of effectiveness and success in the CT domain. Acknowledging the aforementioned pitfalls of policy transfer through tailor-made, environment-specific good practices, the contributors to this project utilized a multi-level approach that integrates i) candidate good alternative models, substantiated and/or not (yet) substantiated by data ii) field-tested good methods, techniques, strategies and procedures that improved the maturity of CT policies and iii) evidence-based/proven good practices that are determined to be the best approach in multiple settings. We consider that these cross-cutting observations, drawn out of the lessons learned through policy evaluations, will at the same time enable multi-sectoral cooperation and bridge the gap between academia and the civilian and military bureaucracy.

Conclusion

Although the disruption in framing terrorism has been moderated somewhat since the September 11, 2001 trauma, we have a long way to go to achieve a universally acknowledged definition of terrorism. However, we cannot deny the progress made in achieving a universal awareness of the brutality of terrorist activities taking place on the stage of everyday life. Meeting on the common ground about the political, economic, and socio-psychological devastations posed by new-age terrorists, states and international security actors have placed CT at the top of their security agendas. This political acknowledgement now manifests itself in many aspects of public policy making. Today, governments have to take into account multiple possible crisis scenarios posed by terrorist networks, while at the same time they

are also shaping a variety of public policies such as critical infrastructure investments, digitalization of state, renovation of military industry, media and communication regulations, storage of hazardous materials, and so on.

Like many other socio-political challenges, we do not have a silver bullet to deal with contemporary terrorism. The only substantiated method to deal with terrorism is to counter it in a comprehensive way against every manifestation of it. Partial or relative success in CT will not guarantee the end of the terrorist threat. Absolute success is dependent on a comprehensive evolution of a CT framework through increased political ownership, reinforcement of societal resilience, professionalization of risk management systems, and multi-sectoral and multi-dimensional strategic cooperation. Learning these lessons through individual national experiences is traumatic and is economically and politically inefficient. To eliminate duplication and guarantee policy efficiency, international community and national level policy makers should draw lessons from good strategies, effective operational approaches and through a diversity of means (hard power, soft power, and smart power) and a variety of "know-how" models drawn out of scholarly produced risk assessment models. This is why we pay special attention to the transfer of "know-how" and the professionalization of CT policies through constant revision of national CT mechanisms which are based on tailor-made good practices. As being the paramount actors in the international system, modern states, which have been successfully organizing CT policies for decades, have required capacity and experience to inspire their international partners. We offer this collection as a unique opportunity for the increasing sophistication of CT policies through documenting and evaluating good practices and maturity models driven out of the success stories that follow.

Bibliography

Bowman, M.E. (2006), "Terrorism Challenges in an Interdependent World." *National Counterterrorism Strategies*, NATO Security through Science Series, pp. 45-57.

Davis, Paul K. and Cragin, Kim (eds.), (2009), *Social Science for Counterterrorism: Putting the Pieces Together*, (Santa Monica, CA: RAND Corporation).

De Graaf, Beatrice (2011), *Evaluating counterterrorism performance: A comparative study*, (London and New York: Routledge).

Freese, Rebecca. (2014) "Evidence-Based Counterterrorism or Flying Blind? How to Understand and Achieve What Works." *Perspectives on Terrorism*, Vol: 8, No: 1, pp. 37–56.

Hoffman, Bruce, (2006), *Inside Terrorism*, (USA: Columbia University Press).

Martini Alice and Njoku E T. (2017), "The Challenges of Defining Terrorism for Counterterrorism Policy", In Scott Nicholas Romaniuk, Francis Grice, Daniela Irrera and Stewart Webb (eds.) *The Palgrave Handbook of Global Counterterrorism Policy*, (London and New York: Palgrave Macmillan), pp. 73-89.

Mueller, John, (2005), "Six Rather Unusual Propositions about Terrorism", T*errorism and Political Violence*, Vol: 17, No: 4, pp. 487-505.

Nalbandov, Robert, (2017), "Evaluating the 'Success' and 'Failure' of Counterterrorism Policy and Practice,'' In Scott Nicholas Romaniuk, Francis Grice, Daniela Irrera and Stewart Webb (eds.) *The*

Palgrave Handbook of Global Counterterrorism Policy, (London and New York: Palgrave Macmillan), pp. 91-115.

NATO Secretary General, (2020), NATO 2030: United for a New Era -Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General-, 25 November 2020, https://www.nato.int/cps/en/natohq/176155.htm (Accessed 12.12.2020)

NATO, (2016), Military Committee Concept for Counter-Terrorism (MC 0472/1 (Final)), 6 January 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160817_160106-mc0472-1-final.pdf (Accessed 12.12.2020)

NATO, (2003), NATO Civil-Military Co-Operation (CIMIC) Doctrine AJP-9, June 2003, https://www.nato.int/ims/docu/ajp-9.pdf (Accessed 12.12.2020)

Richards, Anthony, (2015), Conceptualizing terrorism. (Oxford: Oxford University Press). Sanderson, Ian, (2002), "Evaluation, policy learning and evidence based policy making," *Public Administration*, Vol: 80, No: 1, pp. 1-22.

Schmid, Alex P. (2011), "The Definition of Terrorism," in Alex P. Schmid (ed.), *The Routledge Handbook of Terrorism Research*, (London, New York: Routledge), pp. 57-116.

Schuurman, Bart, (2018), "Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship", *Terrorism and Political Violence*, Vol: 32, No: 5, pp. 1-16.

UN General Assembly, (2015) *Plan of Action to Prevent Violent Extremism, UN General Assembly Resolution A/70/674*.

UN Security Council, (2004), *Security Council Resolution 1566 (2004) on Threats to international peace and security caused by terrorist acts*.

UN, (2006), *Framework for the Collection, Analysis, Development and Dissemination of Best Practices Relative to United Nations Security Council Resolutions 1373 (2001) and 1624 (2005)*.

UN, (2006), *The United Nations Global Counter-Terrorism Strategy, UN General Assembly Resolution* (A/RES/60/288).

CHAPTER II

HARD POWER, SOFT POWER AND SMART POWER CIVILIAN-MILITARY CHALLENGES IN COUNTER-TERRORISM

Stephen Harley

Introduction

Combining hard and soft power approaches to achieve strategic goals is not a new idea. Julius Caesar, during the conquest of Gaul, achieved a decisive military victory over his rival, Vercengetorix, at the battle of Alesia in 52 BCE, the culmination of a back-and-forth campaign that saw Caesar side with one tribe against another, suffer setbacks and see allies turn against him but eventually triumph. As a result, Gaul was subsumed into the Roman Empire.

Caesar's victory in Gaul was not purely an exercise in 'hard', military power, nor for that matter 'hard' diplomacy such as blackmail, coercion, manipulation and bribery. His decisive military victory, and his use of symbolic atrocity such as the amputation of the hands of every fighting age male of the treacherous Ubi tribe or the eventual ritual strangulation of his seeming nemesis, Vercengetorix, in Rome years afterwards, were undeniably 'hard'.[1] But Caesar was equally comfortable with the use of 'soft' approaches too, albeit not quite as 'soft' as we might feel comfortable with today.

Caesar, for example, wrote the story of his campaign in Gaul, 'The Gallic War', close-run-things and all, in the third person: Caesar writing describes Caesar charging into the fray, with his distinctive purple cloak flowing, at times when decisive leadership was required. He also limited the vocabulary of his account to approximately 1300 words, to make the story or, to be accurate, Caesar's version of the story, more accessible beyond the erudite elite, and to make the story more 'transmittable' for orators in public squares, the 'mass media' of the times. This limited-vocabulary account of the defeat of the Gauls was also used as a teaching text: the surviving Gauls were taught Latin using the story of their own recent ignominious defeat. Ultimately many Gauls and other members of conquered races were completely 'Romanised', with a Spaniard, L. Cornelius Balbus, even achieving consulship in 40 BC.[2] That France still has military units called 'Legion' is indicative of how successful Caesar ultimately was. But would this far reaching achievement have been possible if Caesar

[1] Caesar, *The Conquest of Gaul*, Chapter 8, Paragraph 14.
[2] Dr. Lindsay Hall, University of St Andrews, e-mail message to author, 04 September 2020.

had used purely hard power approaches as the Romans had done with a previous adversary, Carthage? Is it not the softer elements of his approach, such as education and social and economic integration that created the enduring effect?

This chapter is about the applicability of the good examples of hard and soft power approaches to counterterrorism, bridging the gap between the considerable body of literature on what constitutes the effective interaction of hard and soft power approaches to achieve foreign policy goals, and the potential role for integrated approaches in achieving the more specific objectives of counterterrorism.

The study of the interaction of hard and soft power approaches, referred to when combined as 'smart power', is still a subject of much academic discussion. However, much of the discourse is focused on foreign policy or on the increasing importance of but also resistance to soft power approaches. Little consideration has been given to implementing these concepts in counterterrorism. As a result, there are few examples of the coordinated, consistent and effective implementation of hard and soft power approaches in unison in counterterrorism.

The chapter firstly explores the developing understanding of what constitutes hard and soft power since the terms were first coined in the early 1990s, and what the integrated use of the two approaches can offer. Examples are given of individual nation states that have successfully used integrated hard and soft power approaches, with specific attention being paid to NATO nations.

The chapter then uses a case study of Somalia, with specific focus on the combination of hard and soft power approaches in the campaign to defeat the al-Qa'ida linked terrorist organization, al-Shabaab, within the broader effort to rebuild the Somali nation state.

The questions this article therefore poses are:

- What is meant by hard power and soft power - and smart power?
- What does good practice mean in the integrated use of hard and soft power out-with the realm of counterterrorism?
- What good practice examples can be drawn out of the integrated use of hard and soft power approaches to counter the terrorist group, al-Shabaab, in Somalia?

The article then concludes with a model for good practice in the use of integrated hard & soft power approaches in counterterrorism and recommendations for future activity, research and otherwise.

Methodology

This chapter uses as its framework a number of short case studies of good practice in the use of hard and soft power and one, more developed study of the use of hard and soft power in counterterrorism as part of the campaign to counter al-Shabaab in Somalia. The chapter approaches these case studies using Bennett & Elman's 'Qualitative Research: Recently Developments in Case Study Methods' as a guide, the key points of which are briefly laid out in this chapter.

One of the fundamental decisions to be made when using case studies is whether to use a 'within case' or 'cross-case comparison' approach.[3] This article makes use of both.

A key element of the methodology of using case studies is explanatory typologies, where the article poses descriptive, classificatory and then explanatory questions about each case study, whether it be the short case-comparisons that explore good practices in hard and soft power out-with the realm of counterterrorism or the longer within-case study of Somalia.

However, Bennett & Elman recognize that a longer case study can yield a depth of insight beyond cross-case comparisons or quantitative methods.[4] In line with this observation, the 'within case' examination of Somalia must meet the following criteria, described as 'Process Tracking': there must be a clear sense of a beginning and an end to the account without substantial gaps, although this does not preclude using events that are still unfolding; the account should suggest evidence and this may Bayesian inference, where effects may be used to identify causes; inconsistent and alternative explanations should be addressed through the observable implications of the evidence presented; and the case study should be conducted in a manner that guards against confirmation bias and other sources of 'skewing'.[5]

To this end, a specific period in Somalia's recent history has been chosen. This period begins in 2007, and the overthrow of the Islamic Courts in Somalia by Ethiopian forces with US backing, which subsequently spawned the nationalist-Islamist terror group, al-Shabaab, as the primary resistance movement to foreign intervention in the country. The period then runs until the present, where al-Shabaab is constrained geographically and financially, but nonetheless continues to operate, albeit with little ability to shape events, and where the institutions of government in Somalia are solidifying and the peaceful transition of power between elected administrations is approaching its second iteration. While the author has been observing, and occasionally deeply involved in, Somali affairs throughout this period, objectivity is assured by consistent referencing of other sources of analysis and opinion, rather than those of the author himself.

In some ways, the case study follows Levy's 'least likely' model, wryly also describe as 'the Sinatra effect': if it can happen here, it can happen anywhere. If Somalia, the world's most dangerous place[6], once the most failed of failed states, although it is now officially 'fragile'[7], and the consistent winner of the dubious title of the world's most corrupt country[8], can show evidence of the effective, integrated use of hard and soft power in counterterrorism, then it seems reasonable to assume that this approach has potential in other theatres.

'Path Selection' is the key element in the effective use of the longer, 'within case' study, and this element identifies 'periods' within the case study. Firstly, there is an open period, where multiple options present themselves, in this instance, the immediate aftermath of the fall of the Islamic Courts Union and the Ethiopian invasion in 2006-2007 until large scale operations by

3 Bennett and Elman, *Qualitative Research*, 473.
4 *Ibid*, p 459.
5 *Ibid*.
6 Ferguson, *The World's Most Dangerous*.
7 Guardian, "Somalia is no longer a failed state, just a fragile one", 23 December 2015.
8 Transparency International, "Global Corruption Perceptions Index 2019", January 2020.

the African Union Mission in Somalia (AMISOM) drove al-Shabaab out of Mogadishu and then continued to harry the group in the rural areas of south/central Somalia. At this point there is a critical juncture (2012-2014), where al-Shabaab was conclusively hemmed into small, rural areas in the Shabelle and Jubba River Valleys and moved primarily to the posture of terrorism, not insurgency. In the same time period the Federal Government of Somalia was formed. Path Selection then focuses on a third period (2014 until the present), where constraints on actors make a move backwards towards previous 'options' less and less likely, albeit with occasional 'reactive sequences', but which do not interrupt the overall passage down along one course. In this third phase consideration is also given to how structures were created and maintained: in the case of this article, this translates into analysis of why a combination of hard and soft power approaches were chosen in the fight against al-Shabaab, as opposed to the previous, exclusively hard power measures.[9]

This approach then allows us to step back from the wider case-comparisons and the specific, within-case study of Somalia, and to draw conclusions about what constitutes goodpractice in the application of smart power in counterterrorism.

Literature Review

At this point it is worthwhile defining exactly what we mean by hard power, soft power and smart power, prior to laying out a number of case comparisons from out-with the realm of counterterrorism but with specific reference to security and/or Somalia.

Definitions

Since Joseph S. Nye first coined the term, 'soft power' in 1990[10], Nye himself has refined and expanded upon the concepts of hard and soft power and then, in 2003, smart power, in response to both criticism and changes to the global order. In 2009 he summed up where his understanding of his own terms was:

> 'Power is one's ability to affect the behavior of others to get what one wants. There are three basic ways to do this: coercion, payment and attraction. Hard power is the use of coercion and payment. Soft power is the ability to obtain preferred outcomes through attraction.'[11]

One critical point for Nye in the development of understanding of the interaction of hard and soft power was the need to clarify the misunderstanding that soft power alone would ultimately replace hard power: this was not the case, he fielded, and introduced the term smart power to emphasize the value of the interaction of the two elements in an integrated manner to achieve effects and, ultimately, objectives.[12] Latterly, Nye has noted a vindication of his ideas in 'the Information Revolution'[13] which we are currently going through, where the high speed transfer of information and ideas has resulted in a broadening of power beyond

[9] Bennett and Elman, *Qualitative Research*, 463-465.
[10] Nye, *Bound to Lead.*
[11] Nye, *Get Smart*, 161.
[12] Ibid.
[13] Nye, *The Information Revolution*, 19.

the traditional, 'old' industrial powers. Nye sees 'old' powers as typified in groups such as the G8. However, power now also lies with smaller and emerging nation states, private companies and non-state actors including terrorist groups and organized crime cartels. The Information Revolution, Nye asserts, has also allowed delegation of the ability to message and influence potentially to the lowest common denominator of an individual with a smartphone in his or her pocket, regardless of where they are in the world.[14]

There have been numerous critiques and challenges to Nye. Wilson, for instance, asks whether Nye's theories are too US-centric, too focused on a large, enormously wealthy, historically hard power oriented country. He also preempts Nye's recognition of the effects of 'the Information Revolution' by redefining power as:

> 'A nation's capacity to create and manipulate knowledge and information. A nation's capacity for creativity and innovation can trump its possession of armored divisions or aircraft carriers, and new hi-tech tools can greatly enhance the reach of military and non-military influence'[15]

This is clearly a divergence from Nye's conception: Wilson is asserting that Soft Power can, on some occasions, and perhaps will, at some point in the future, usurp the dominance of Hard Power.

Wilson also focuses on the difficulties of implementing Smart Power, noting the continuing dominance of Hard Power tools in terms of budget, personnel and likelihood of use. He compares the 2008 budgets of the US Departments of Defense ($260 billion) and the US Department of State ($10 billion, of which only $1.5 million is actually allocated to influence activities) and describes the consistent denigration of US Soft Power assets such as the Department of State, USAID and the sadly defunct United States Information Agency (USIA). He notes that the hard power proponents still have 'the Power', while soft power remains an occasional afterthought or an academic exercise.[16]

In terms of what practically constitutes 'Hard' and 'Soft' Power, a distillation of the available literature is shown in the table below.

Hard Power	**Soft Power**
Military	Development/Aid including Infrastructure
Economic	Education
Diplomatic	Culture & the Arts
Legal	Sport
Policing	Tourism
	Religion/Philosophy
	Information

Table 1: The Elements of Hard & Soft Power

[14] Ibid, 19-21.
[15] Wilson III, *Hard Power, Soft Power*, 112.
[16] Ibid, 116-122.

But this rigid delineation does not reflect the reality that some disciplines stretch across the spectrum of Hard and Soft Power. Military power, for example, is at its 'hardest' when it involves the threat of or actual war. At a lower level, strikes can be conducted against states or non-state actors such as terrorist groups without a state of war being declared. Specific targets can be targeted using air-power, be they manned aircraft, drones or precision munitions, or Special Forces, sometimes in a deniable manner. With specific reference to counterterrorism, the deployment of the military in what the UK calls 'Military Aid to the Civil Authorities' (MACA) in the 'maintenance of law, order and public safety using specialist capabilities or equipment beyond that of the Civil Power'[17], saw troops patrolling alongside the police force during the Troubles in Northern Ireland. This has been revisited on the UK mainland during recent peaks in terrorist activities such as during the aftermath of the Manchester Arena bombing and the London Borough Market attack.[18]

But military power could also include a contribution to a UN Peacekeeping Mission, where the hard power is more related to the presence and the potential threat of military power, rather than the actual application of force. It could also see the deployment of medical personnel, engineers and other non-combat elements of the armed forces in the aftermath of a natural calamity such as a hurricane. Alternatively, using the military's unique combination of relevant skills and its ability to operate in arduous environments, along with its rapid deployability makes it a potentially very useful soft power tool. There is also its 'off the shelf' availability: that is the nature of a standing force.

Economic power, too, might mean a 'hard' approach such as interrupting the flow of energy, a scenario which prompted tense discussions between the Germany and US governments over the Russian Nord Stream 2 in August 2020, or restricting tourism to partner state that is proving non-compliant[19] such as the Russian restrictions on tourist flights to Turkey in the aftermath of the accidental downing of a Russian fighter plane in December 2015. But it could also mean an easing of immigration restrictions, as the UK has done with Commonwealth countries such as Kenya in the aftermath of Brexit[20], or deliberate support in the form of investment in a country whose support the 'powerful' nation seeks in other arenas, such as votes in the UN and so on. This an approach that China has used extensively with its African partners[21].

A more accurate representation, then, might instead not show merely two columns of Power, Hard and Soft, but instead a spectrum across which the various approaches extend.

---

17 UK Ministry of Defence, "2010 to 2015 government policy: armed forces support for activities in the UK", 08 May 2015.

18 "Soldiers deployed on streets in race to foil second terror attack after threat level raised to critical", *Daily Telegraph*, 24 May 2017; Phipps et al., "Soldiers on British streets as threat level raised to critical – as it happened", *The Guardian,* 24 May 2017.

19 "Germany expresses 'displeasure' at US threat over Russia pipeline", *Al Jazeera*, 10 August 2020; "Moscow's flight ban hits Turkish tourism industry", *Financial* Times, 17 December 2015,

20 "UK offers work permit to non-graduate Kenyans", *Business Daily Africa*, 14 July 2020,

21 Servant, *China steps.* ; Green, *Did China Stoke.*

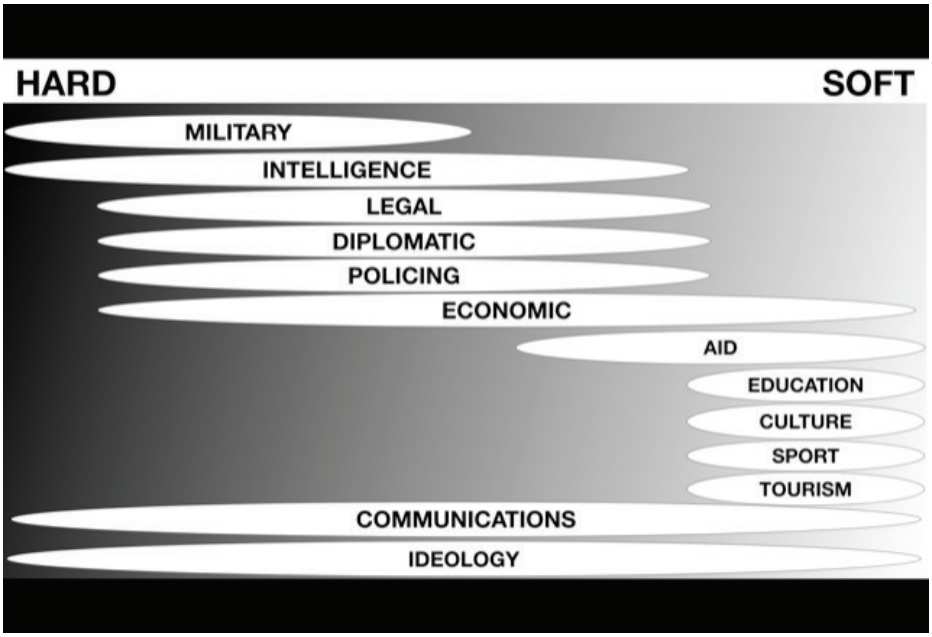


Figure 1: Spectrum of Hard and Soft Power Activities

Good Practices Survey of Hard-Soft Power Interactions

The most recent studies of hard and soft power combining to achieve smart power are more hopeful than the review of the academic literature might suggest. While noting once again the dearth of literature on hard and soft power approaches which directly reference counterterrorism, there are some valuable studies of some countries, both 'old' and 'emerging' powers, that provide useful, if slightly broader examples. For the purposes of focus, this section examines ways of measuring power using two primary mechanisms: the Webber Shandwick 'Future Brand Country Index' and the Monocle magazine 'Soft Power Survey'. This allows a broad assessment of the effectiveness of various nations in using approaches other than hard power. However, and once again to maintain focus within the limited scope of this chapter, countries which also make use of hard power or which have adapted their existing hard power components are given most attention in this section, since these will then be most relevant to the subsequent study of counterterrorism in Somalia.

The 'Future Country Brand Index 2019' begins:

> 'Countries have traditionally been measured and ranked by measures of might - GDP, population size, even a sovereign's nuclear arsenal. However, in the current day, when our world is defined by rapid change, do these measures make sense in the ranking of nations?'[22]

[22] Shandwick, *Future Brand*, 5.

Monocle poses a similar question, but notes that while most nations meticulously measure hard power capacity in terms of numbers of troops, tanks and planes and so on, there is no parallel intra-national audit of soft power.[23] Both products attempt to address this deficit and come to the same broad conclusions about what makes a successful soft power country, even to the extent of consistently choosing the same countries in their 'Top Ten': Australia & New Zealand, Canada, Germany, Japan, the Scandinavian nations and Switzerland. Elements such as the number of tourists and foreign students feature heavily, as does a strong diplomatic presence abroad and programmes of international aid and development.[24] The Future Brand Country Index also emphasizes quality of life, environmental friendliness and the national 'brand' as core components of soft power success, along with 'values' and a healthy and free communications environment.[25] It is noted, however, that soft power success may be compromised in a number of ways, usually by hard power.

Of particular interest to this study are countries that have strong profiles in the both the hard and soft power arenas: Denmark, Norway and Turkey. Denmark, for example, is viewed as a soft power success because of its culture, ranging from literature and television drama to the Danish way of life. Its liberal values are also a strong point, although this has been compromised in Monocle's view by its recent posture on immigration[26]. It has, nonetheless, a powerful naval capability in support of its maritime industry, a significant element of its economic might, within a small but highly regarded armed forces. The Royal Danish Navy's contribution to the NATO and EU counter piracy blockades off the coast of Somalia is highlighted in Monocle's How to Build a Nation, which notes that it is 'progressive' and 'egalitarian'[27] but at the same time has a contingent of *Fromandkorpset,* Denmark's Tier 1 maritime Special Forces, on board a highly sophisticated warship.

Norway, similarly, has strong soft power credibility with its culture and scenery rated highly in online references and with a strong reputation for its commitment to the environment, despite its reliance on the fossil fuel industry[28]. But it is also an exemplary case study in the way it has adapted its military to become both a hard and a soft power tool. Its national service officer training programme, for example, is highly selective and, while arduous, it emphasises character and intellectual capacity: the result is a qualification that is highly prized not just in the Norwegian military but across Norwegian society and which is recognized as being amongst the best officer training programmes in the world. Integral to the course are scenarios that range from conventional warfare to humanitarian disaster relief. The latter are components that are often covered in other armies when they arise, as opposed to being viewed as part and parcel of the military's capability, as Norway does. This has created an effective military force that is highly capable across the spectrum of

23 Monocle, *How to Make a Nation,* 22.

24 Monocle magazine, "Power Play: 2016 Soft Power Survey", Vol. 90, December 2016 - January 2017, pp. 51-59; Monocle, "Softly Does It: 2017 Soft Power Survey", Vol. 10, December 2017 - January 2018, pp. 51-59; Monocle, "Soft Power Survey 2018/2019", https://monocle.com/film/affairs/soft-power-survey-2018-19/.

25 Shandwick, *Future Brand*, 29-48.

26 Monocle magazine, "Softly Does It: 2017 Soft Power Survey", December 2017 - January 2018, 56.

27 *Ibid*.

28 Shandwick, *Future Brand*, 69.

conflict.[29] It does, of course, have a tangible, looming threat on its northern borders in the form of Russia, which provides a very real world focus for Norway. But in many ways the Norwegian military is the epitome of a smart power armed forces.

Turkey is another example of a nation that wields a combination of hard and soft power. A notable example of the former is Turkey's leadership in the military campaign against ISIS/Da'esh in Syria[30]. But Turkey is also building on its previous success in the integration of hard and soft power approaches in Afghanistan. While part of the ISAF mission, Turkey deployed a military presence, but this was supported by multiple soft power approaches: religious and cultural affinity; tangible soft power engagement in the form of education, both in country and through scholarships to study in Turkey itself; infrastructure development; and direct aid[31].

But in Somalia, Turkey has given soft, not hard power tools prominence. Recent public perception polling in Somalia consistently identifies Turkey as the largest international donor, whereas recent data shows it is in fact somewhere between the 5th and 11th[32], a testament to the effort Turkey has put into publicizing its activities but also targeting its activities on areas of publicly-identified need. Mogadishu Airport, Mogadishu Seaport, roads, medical facilities and schools are all examples of this. Turkey also emphasizes its willingness to operate in the city of Mogadishu, not confining itself to Mogadishu International Airport, where much of the international community presence resides. Turkey's prominent embassy is sited on the city's Lido Beach and Turkish airport and seaport staff live in the city and worship in local mosques.[33]

Similarly, Turkey has integrated its national flag carrier, Turkish Airlines, into its overall effort: Turkish Airlines was the first non-African carrier to establish regular flights to Mogadishu, and aircraft are regularly repurposed to deliver aid or transport the victims of terrorist atrocities to Turkey for treatment.[34] It is interesting to note, however, that Turkey's recent engagement in security sector reform has resulted in direct targeting by al-Shabaab. Turkey is, nonetheless, the embodiment of a country that has fully integrated its hard and soft power tools into a smart whole, with the overall emphasis on the soft. It is an example of good practice in this regard.

Some Conclusions about Hard & Soft Power Interaction

The concept of hard and soft power combining to achieve smart power is by no means yet the norm. But the countries that provide us with examples of good practices have found success in this realm by placing soft power to the fore and have proven to be adaptive with their existing tools of influence, including the military. Those countries have also shown

---

29 Monocle, *How to Make a Nation,* 108-113.

30 "Turkey is a leading NATO member, it's time this commitment was recognized", *Euronews*, 29 November 2019.

31 Sey and Seufert, *Turkey in Afghanistan*, 1-4.

32 UNDP, "Aid Flows in Somalia", April 2017, https://www.undp.org/content/dam/unct/somalia/docs/publications/Aid%20Flows%20Booklet%20FINAL.pdf.

33 Sazak and Woods, *Thinking Outside.*

34 "Turkish Airlines Gives Back; Teams Up with Social Media Celebrities to Fight Famine and Drought in Somalia", *PR Newswire*, 17 August 2017; "Turkey evacuates wounded after deadly Mogadishu blast", *Reuters,* 29 December 2019.

cultural openness or found areas of affinity and are willing to be, to a certain extent, 'led' by local needs rather than international agendas. They do, nonetheless, still ultimately conform with that agenda, but they are also committed and consistent.

But it must be remembered that smart power can be precarious and the entire effort can be undermined very quickly by dissonant hard power efforts. Nye himself notes the damage to the reputation of the US that the Global War on Terror caused and goes onto to highlight how the deployment of soft power approaches will neither mitigate nor distract from hard, nefarious activities elsewhere. Nye and Monocle's How to Build a Nation both reference the examples of Russia and China's attempts to establish 'independent' English-language international news outlets to further their national agendas in the form of RT and CCTV: but both are rightly viewed around the world as being little more than clumsy propaganda channels.[35]

Case Study: Hard and Soft Power Counterterrorism Approaches in Somalia

The focus of this chapter now shifts to Somalia, and the integrated use of hard and soft power to counter the activities of the al-Qa'ida affiliated terror group, al-Shabaab.

Uses of Hard Power to Counter al-Shabaab

There is a clear 'hard' component to the campaign against al-Shabaab in Somalia: the frequency of US drone strikes alone gives a clear indication of that[36] and, at the time of writing, that frequency is actually increasing[37]. Special Forces raids and conventional operations to recover rural towns and villages from al-Shabaab control, conducted by the Somalia National Army (SNA) with support from the African Union forces and international advisors are also a regular occurrence. There is also an extensive international training effort involving the United States, the United Kingdom, the European Union and Turkey. But, as noted before, hard power brings an implicit risk of compromise, and there is an increasing focus on the inevitable civilian casualties that result.[38]

There is also a network of diplomatic sanctions and legal measures in place to constrain the activities of al-Shabaab. These range from limitations on the import of weapons and other military equipment, travel bans, anti-terror financing and international funds transfer controls, the listing of specific individuals and organizations and even bounties for the killing or capture of high profile commanders in the group. Some of these are applied by the UN Security Council[39], some by individual nation actors, such as the US's Rewards for Justice List.[40]

---

35 Nye, *The Information Revolution*, 19-22; Monocle, *How to Make a Nation,* 193.

36 "Somalia: Reported US Actions 2019", *Bureau of Investigative Journalism*, 2019*,* https://www.thebureauinvestigates.com/drone-war/data/somalia-reported-us-actions-2019-strike-logs.

37 Turse, *US hit.*

38 Turse, *The Trump Administration's.*

39 United Nations Security Council, "Sanctions in Place to Help Somalia Government Confront Terrorism, Restore Stability, Speakers in Security Council Stress", 27 February 2020.

40 U.S. Department of State "Rewards for Justice - al-Shabaab Leaders Reward Offers", Office of the Spokesperson*,* 07 June 2012, https://2009-2017.state.gov/r/pa/prs/ps/2012/06/191914.htm.

Furthermore, in a country where the justice system is still lacking in transparency and challenged by traditional mechanisms of dispute resolution, terrorist cases are 'fast-tracked' through the Military Courts. There is also an extensive security apparatus beyond the SNA, including the National Intelligence & Security Agency (NISA) and the Somali Police Force (SPF), which deploys checkpoints, conducts forensic analysis after attacks and gathers intelligence, all with the support of the international community. The Somali government frequently messages about its counter al-Shabaab operations through its Ministry of Information and the various state broadcasters. That said, this is with a distinctly 'hard' approach - bloody images of dead al-Shabaab fighters are the norm.

This is often where a counterterrorism campaign ends, with an array of hard power approaches - and all the associated risks to the reputation and the integrity of the mission. Not so in Somalia.

Uses of Soft Power to Counter al-Shabaab

The remainder of this section focuses on two, broadly linked soft power approaches: negotiated settlement, supported by public diplomacy, and reconciliation, including the Disarmament, Demobilization and Reintegration (DDR) process.

The defection in June 2013 of the former leader of the Islamic Courts Union and senior al-Shabaab ideologue, Sheikh Hassan Dahir Aweys, was a major coup for the then Transitional Federal Government of Somalia. However, the aftermath of his defection, was messy. Firstly, there was the humiliating circumstances of his transportation to Mogadishu: despite being a terrorist, he was also an elderly, respected cleric and did not deserve such treatment, many felt. Secondly, at times he refused to renounce either violence, Radical Islam or anti-westernism, mentioning only al-Shabaab as the group he was rejecting. His defection was also undermined by his unchecked statements to the media, which loudly aired his grievances. As a result, the Somali government sought support from the international diplomatic community in managing high level defections in the first instance and a broader process of negotiated settlement.

The resulting UK-funded programme, 'High Level Defections' (HLD), ran in parallel to a variety of programmes that handled low level defectors. Some of the low level programmes were internationally supported, others were organic and based on clan 'vouchsafes' for defectors.

But it was recognized that commanders would be a different proposition to foot-soldiers. They have more to offer in terms of actionable intelligence and broader insight. They also had an expectation of status and reward when they defected and were often high-status individuals within Somalia's clan system anyway. They had networks which were probably still active within al-Shabaab, offering the chance of more defectors. But they were often subject to sanctions or listed on the various bounty programmes. They also offered a far

greater yield in terms of the damage a high profile defector can do to perceptions of a terror group, but the publicity around their defections would have to be very carefully managed.

Public Diplomacy, led by British Embassy Mogadishu, was therefore engaged to de-list defectors such as Atom (defected June 2014), Zakariye (December 2014) and Robow (August 2017), whether it be engaging with the UN to remove sanctions or the US to withdraw the individual from the Rewards for Justice programme. There were more than 80 other defections by al-Shabaab commanders in the period of the HLD programme, June 2014 - June 2018, although none of those individuals were subject to sanctions. This process was supported by extensive media coverage at the national and international level.[41]

Above the level of individual commanders, there have been attempts to engage with al-Shabaab towards a negotiated settlement (2008 and 2011) but these have not proved successful, often because al-Shabaab refuses to recognize or engage with the Somali government. At the time of writing, however, Somali government and the international community are exploring the possibility of finding a suitable, ideally Muslim intermediary that is acceptable to all parties. Pakistan and Indonesia have both been suggested, since most Middle Eastern or North African countries have a stake of some sorts in Somalia or are viewed by al-Shabaab as being 'apostates'.

At the level of the foot-soldier, a different kind of soft power approach has been used. This approach challenged what defectors had been told to expect by al-Shabaab commanders: they would be put against a wall and shot by African Union or SNA soldiers. Instead, a combination of soft power approaches are offered with the emphasis on the Reintegration component of the DDR process. In the Serendi Defector Rehabilitation Centre (DRC) in Mogadishu, religious scholars clarify misconceptions about the Quran, teachers fill in the gaps in education, skills such as tailoring and vehicle maintenance are taught and there is an extensive programme of sports on offer. There is a post-care business development programme that offers micro-finance, funded by Japan. Those requiring assistance in dealing with trauma see social workers and counsellors and those with medical issues are treated.[42] Other DRCs operate as Kismayo and Baidoa as well.

In parallel, in the Elman Peace & Human Rights Centre in Mogadishu, former child soldiers go through a similar process, but with even more emphasis on mental health and general well-being, including yoga classes on the beach.[43] The DRCs are supported by international donors such as the UK, Denmark and the International Organization for Migration, while the programmed support to former child combatants is provided by UNICEF, showing another form of soft power interaction in a counterterrorism campaign, that of international coordination through diplomacy.

---

41 Harding, *Somali defector*; "Exclusive: Somalia lures defectors in new push against insurgents" *Reuters*, 24 January 2018.

42 Taarnby, *Serendi*.

43 Elman Peace, http://elmanpeace.org.

But is it Smart?

There are clearly a range of hard and soft power approaches being used to counter al-Shabaab in Somalia. But a perennial danger in counterterrorism, and in any 'expeditionary' engagements outside a nation's own borders or region, is of actors operating in isolation. While Somalia is not immune to this by any means and, in fact, unilateral action is widespread, in the realm of counterterrorism there is a significant degree of coordination and cooperation, led by Public Diplomacy. With regard to countering al-Shabaab at least, the use of hard and soft power is definitely 'smart'.

For example, at the beginning of the HLD programme, three countries, Turkey, the UK and the US, would meet periodically in a forum known as 'The Troika', to discuss ways to counter al-Shabaab. At the time those country's diplomats felt, quite rightly, that they were the main 'players' in counterterrorism. A specific example of how this diplomatic effort supported the counterterrorism effort was the sharing by UK diplomats of the list of those being engaged as potential defectors by the HLD programme with the US, to ensure that those names did not also appear on targeting lists for strikes.

Soon three became six, and 'The Secretariat' was formed. Latterly it was recognized that international institutions such as the United Nations, the African Union and the European Union also need to be involved in the ongoing conversation. Subsequently efforts were made to ensure that the stabilization and humanitarian elements of the international community should be involved in the discussion as well. Some nations have chosen to remain anonymous in their activities, apportioning attribution to the Somali government: others publicize their role openly.

As one senior international advisor currently working in Somalia comments, 'I need a meeting to coordinate my meetings.'[44] But the effort to coordinate is nonetheless an attempt to ensure that the myriad of activities going on in Somalia, hard and soft, are being delivered in a 'smart' fashion.

This is not to say that there have not been challenges: al-Shabaab, for example, was not passive in the face of the damaging effort to lure disaffected members out of the organization, imposing vigorous security restrictions and actively targeting defectors. Two defectors turned 'outreachers' were killed while trying to persuade others to follow them out of the group. It must always be remembered that the adversary also has a say, and can also use both soft and hard power approaches itself. Al-Shabaab puts a great deal of effort into publicizing its system of courts, medical care, and education, for example, not just its attacks.

At the same time, the concepts around defection, negotiated settlement and so on were not socialized with the population. In a focus group testing of a video product about the Serendi centre, participants were hostile:

[44] Senior security sector advisor, special interview with the author, 03 September 2020.

> "They joined al-Shabaab under their own volition and have participated in violent acts including killing of Muslims, women and children… They shouldn't be given special treatment."[45]

Or, more simply:

> "Hang them. Kill them."[46]

Fortunately, after viewing the product they changed their view, but the critical soft power element of communications was seriously neglected and was too often an afterthought.

In conclusion, while the example of the use of hard and soft power counterterrorism approaches in Somalia is by no means perfect, we return to Levy's justification for a 'Least Likely' case study model: if it can happen there, it can potentially happen anywhere.

Conclusion

The integrated use of good practices in hard and soft power to achieve smart power remains the exception rather than the rule, primarily because of the continuing predominance of hard power proponents in positions of influence and in charge of large budgets. The lack of understanding of what soft power constitutes is slowly being addressed, but few nations actually audit their soft power potential in the same way they do their hard power.

However, some nations do understand the value of using hard and soft power approaches in interaction to achieve smart power and national objectives, resulting in a number of examples of good practices that other countries could learn from. That said, these are still relatively limited in number.

But there is no reason why other countries cannot do this, as long as they have a system of values at their core that allows for the credible use of soft power. Nor is there any reason why international organizations such as NATO, along with the United Nations, the European Union, the African Union et al, cannot either, especially given the various grandiose charters that are at the core of each. In particular, military power can be adapted to soft power functions, but this a choice that some nations choose not to make. Other functionaries of government, such as diplomats, the intelligence community and those involved in the law such as lawyers and the police, and economics seem to find it considerably easier to move between a hard and soft stance.

There are, though, some important conditions to be considered in the design of a smart power effort that follows good practices, especially if it is in the realm of counterterrorism.

Firstly, choose the 'face' of the campaign carefully. In an international environment, a degree of national and organizational self-awareness will be important: some countries will have a cultural affinity and should be overt in their engagement, others will be culturally discordant and their presence should be minimal or even covert. A former colonial power, for

[45] British Embassy Mogadishu HLD Programme Report, "22MAY18 Be Amongst Your People Focus Group Results".

[46] Ibid.

example, may not make the best 'lead' in an international campaign when there is perhaps a 'new' country that would be a more palatable option. In the case of Somalia, the African Union Mission includes troops from only one Muslim country and that country, Djibouti, does not lead the mission. With the benefit of hindsight a better option may have been to recruit from Muslim African countries, or form the mission from out-with Africa, since many Somalis feel more affinity with the Gulf. This will be especially important if the terrorist group is strongly ethno-nationalist and/or religious. Both are the case with al-Shabaab.

Secondly, coordination is essential. While this is hardly a revelation, coordinating with the stabilization and humanitarian sectors might be very new for some, especially traditional hard power actors. But this can yield results in an integrated, 'smart' counterterrorism campaign.

Thirdly, in smart power, soft power leads. This may mean that the individual 'face' of a mission wears a suit, not a uniform. Perhaps he or she might even wear a t-shirt. The 'face' may be local, with attribution of activities always going to the local government or local actors. This requires national-level humility. It means the practice of sticking prominent flags and badges on everything and flooding the media with back-slapping videos may have to be put aside until the terrorist threat is diminished because every one of those flags and badges is potentially a magnet for a terrorist attack. Or possibly put aside forever, the ultimate show of modesty.

Fourthly, communication is vital and must take place before during and after every activity, to shape, sustain and where necessary, react. Dr David Kilcullen has observed that terrorists also use hard and soft power, which he sees as typified in information warfare, but that their balance is 10% operations/90% communication[47]. The balance appears to be the opposite with those fighting terrorists and insurgents.

Communication must be built into all activities, not sit as a separate entity, and it must be credible, and again this will generally mean local. Democratic institutions change direction in the manner of a supertanker, not a speedboat. Shifting the balance will inevitably be gradual. Perhaps moving to a 50/50 balance in command structures between the military and the civilian, be it political, diplomatic or aid, would be a good first step that can then cascade downwards through the counterterrorism mission. This may require the civilian side to accept more risk - or look more to the private sector.

This chapter is limited in scope, with only three short and one long case studies, only that latter of which is focused purely on counterterrorism. There is a requirement for more study of the examples there are of hard and soft power in counterterrorism, such as the latter years of the Troubles in Northern Ireland or the campaign against the FARC in Colombia. There may also be scope for more modelling of 'what if we had...?' scenarios to explore how soft power could have been used in what were exclusively hard counterterrorism campaigns. NATO could also begin by auditing its own soft power components and tracking how those components currently interact with hard power.

---

[47] David Kilcullen quoted by Sam Worby in "Influence Operations as Counterinsurgency: A Strategy of Divisiveness", *Cornell International Affairs Review,* Vol. 3, No. 2, 2010, 1-21.

Clearly there is much to be done to adapt existing organizational counterterrorism structures to achieve good practices through the smart power approach: but the examples of how to do it are certainly there and are undoubtedly transferrable to the realm of counterterrorism.

Bibliography

Al Jazeera, (2020), "Germany expresses 'displeasure' at US threat over Russia pipeline", 10 August 2020, https://www.aljazeera.com/news/2020/08/germany-expresses-displeasure-threat-russia-pipeline-200810120206513.html. (Accessed 15 December 2020).

Bennett, Andrew and Elman, Colin, (2006), "Qualitative Research: Recent Developments in Case Study Methods", *The Annual Review of Political Science*, Vol. 9, pp. 455-476.

Business Daily Africa, (2020), "UK offers work permit to non-graduate Kenyans", 14 July 2020, https://www.businessdailyafrica.com/economy/UK-offers-work-permit-to-non-graduate-Kenyans/3946234-5592762-7ala6mz/index.html. (Accessed 15 December 2020)

British Embassy Mogadishu High Level Defectors Programme, "22MAY18 Be Amongst Your People Focus Group Results".

Bureau of Investigative Journalism, (2019), "Somalia: Reported US Actions 2019", https://www.thebureauinvestigates.com/drone-war/data/somalia-reported-us-actions-2019-strike-logs. (Accessed 15 December 2020)

Caesar, Julius, (1951), *The Conquest of Gaul*, trans. S.A. Hanford, (London: Penguin).

Daily Telegraph, (2017), "Soldiers deployed on streets in race to foil second terror attack after threat level raised to critical", 24 May 2017, https://www.telegraph.co.uk/news/2017/05/23/theresa-may-increases-uk-terrorist-alert-critical-manchester/. (Accessed 15 December 2020)

Euronews, (2019), "Turkey is a leading NATO member, it's time this commitment was recognized", 29 November 2019, https://www.euronews.com/2019/11/29/turkey-is-a-leading-nato-member-it-s-time-this-commitment-was-recognised-view. (Accessed 15 December 2020)

Ferguson, James, (2013), *The World's Most Dangerous Place: Inside the Outlaw State of Somali*, (United Kingdom: Bantam Press).

Fields, Nic, (2014), *Alesia 52BC: The Final Struggle for Gaul*, (UK: Osprey).

Financial Times, (2015), "Moscow's flight ban hits Turkish tourism industry", 17 December 2015, https://www.ft.com/content/6146d0e6-9f5b-11e5-beba-5e33e2b79e46. (Accessed 15 December 2020)

Green, Andrew, (2020), "Did China Stoke a Heated African Race for a U.N. Security Council Seat?", *World Politics Review,* 19 June 2020, https://www.worldpoliticsreview.com/trend-lines/28856/did-china-stoke-a-heated-african-race-for-a-u-n-security-council-seat. (Accessed 15 December 2020)

Harding, Andrew, (2015), "Somali defector: Why I left al-Shabab", *BBC,* 19 May 2015, https://www.bbc.com/news/world-africa-32791713. (Accessed 15 December 2020)

Mitchison, Naomi (1927), *The Conquered,* (UK: The Traveller's Library)

Monocle, (2018), "Soft Power Survey 2018/2019", 21 December 2018, https://monocle.com/film/affairs/soft-power-survey-2018-19/. (Accessed 15 December 2020)

Monocle (2016), *How to Make a Nation: A Monocle Guide*, (Berlin: Gestalten).

Monocle, (2017), "Power Play: 2016 Soft Power Survey", Vol. 90, pp. 51-59.

Monocle, (2018), "Softly Does It: 2017 Soft Power Survey", Vol. 109, pp. 51-59.

Nye, Joseph S., (2014), "The Information Revolution and Soft Power", *Current History*, Vol. 113, No. 759, pp. 19-22.

Nye, Joseph S., (2011), *The Future of Power,* (New York: Public Affairs Books).

Nye, Joseph S., (2009), "Get Smart: Combining Hard and Soft Power", *Foreign Affairs*, July/August 2009, https://www.foreignaffairs.com/articles/2009-07-01/get-smart. (Accessed 15 December 2020)

Nye, Joseph S., (March 2008), "Public Diplomacy and Soft Power", *The Annals of the American Academy of Politics and Social Science*, Vol. 616, pp. 94-109.

Nye, Joseph S., (1990), *Bound to Lead: The Changing Nature of American Power,* (New York: Basic Books).

Phipps, Claire, Rawlinson, Kevin, Weaver, Matthew, Sparrow, Andrew and Johnston, Chris, (2017), "Soldiers on British streets as threat level raised to critical – as it happened", *The Guardian,* 30 May 2017, https://www.theguardian.com/uk-news/live/2017/may/22/manchester-arena-ariana-grande-concert-explosion-england. (Accessed 15 December 2020)

PR Newswire, (2017), "Turkish Airlines Gives Back; Teams Up with Social Media Celebrities to Fight Famine and Drought in Somalia", 17 August 2017, https://www.prnewswire.com/news-releases/turkish-airlines-gives-back-teams-up-with-social-media-celebrities-to-fight-famine-and-drought-in-somalia-640897743.html. (Accessed 15 December 2020)

Reuters, (2019), "Turkey evacuates wounded after deadly Mogadishu blast", 29 December 2019, https://www.reuters.com/article/us-somalia-blast/turkey-evacuates-wounded-after-deadly-mogadishu-blast-idUSKBN1YX06C. (Accessed 15 December 2020)

Sazak, Onur and Woods, Auveen Elizabeth, (2017), "Thinking Outside the Compound: Turkey's Approach to Peacebuilding in Somalia", in Charles T. Call and Cedric De Coning (eds.), *Rising Powers and Peacebuilding,* (Manchester: Palgrave Macmillan).

Servant, Jean Christophe, (2019), "China steps in as Zambia runs out of loan options", *The Guardian,* 11 December 2019, https://www.theguardian.com/global-development/2019/dec/11/china-steps-in-as-zambia-runs-out-of-loan-options. (Accessed 15 December 2020);

Sey, Cem and Seufert, Gunther, (May 2016), "Turkey in Afghanistan", *Stiftung Wissenschaft und Politik*, https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C28_sey_srt.pdf. (Accessed 15 December 2020)

Taarnby, Michael, (2018), *Serendi: Inside Somalia's Terrorist Rehabilitation Project,* (Paperback Edition).

Guardian, (2015), "Somalia is no longer a failed state, just a fragile one", 23 December 2015, https://www.theguardian.com/world/2015/dec/23/somalia-no-longer-a-failed-state-just-a-fragile-one-says-un (Accessed 15 December 2020)

Transparency International, (2020), "Global Corruption Perceptions Index 2019", https://www.transparency.org/files/content/pages/2019_CPI_Report_EN.pdf, Accessed 15 December 2020

Turse, Nick, (2020), "The Trump Administration's Air Strikes in Somalia Are On the Rise Again—and Civilians Are Paying the Price", *Time,* 14 August 2020, https://time.com/5879354/civilian-deaths-airstrikes-somalia/, (Accessed 15 December 2020)

Turse, Nick, (2020), "US hit all time high as coronavirus spreads in Somalia", *The Intercept*, 22 April 2020 https://theintercept.com/2020/04/22/coronavirus-somalia-airstrikes/. (Accessed 15 December 2020)

UK Ministry of Defence, (2015), "2010 to 2015 government policy: armed forces support for activities in the UK", 08 May 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-armed-forces-support-for-activities-in-the-uk/2010-to-2015-government-policy-armed-forces-support-for-activities-in-the-uk (Accessed 15 December 2020)

UNDP, (2017), "Aid Flows in Somalia", https://www.undp.org/content/dam/unct/somalia/docs/publications/Aid%20Flows%20Booklet%20FINAL.pdf. (Accessed 15 December 2020)

US Department of State, (2012), "Rewards for Justice - al-Shabaab Leaders Reward Offers", Office of the Spokesperson, 07 June 2012, https://2009-2017.state.gov/r/pa/prs/ps/2012/06/191914.htm (Accessed 15 December 2020)

Shandwick, Webber, (2019), **"**Future Brand Country Index 2019 (2019)", https://www.futurebrand.com/futurebrand-country-index. (Accessed 15 December 2020)

Wilson III, Ernest J., (2008), "Hard Power, Soft Power, Smart Power", *The Annals of the American Academy of Politics and Social Science,* Vol. 616.

Worby, Sam, (2010), "Influence Operations as Counterinsurgency: A Strategy of Divisiveness", *Cornell International Affairs Review,* Vol.3, No. 2, pp. 1-21.

CHAPTER III

"NOT IF, BUT WHEN": DEVELOPING NATIONAL COUNTER-TERRORISM POLICY IN THE AGE OF AL-QAEDA AND ISIS

Susan Sim

A National Security Imperative

In developing national counterterrorism policies, governments often have to deal with a conundrum: How do states carry out effective counterterrorism without increasing the sense of insecurity among a public that is already very concerned about terrorist attacks? The Spring 2020 Global Attitudes Survey[1] by the Pew Research Center shows many citizens in Europe, North America and East Asia consider terrorism to be among the top three global threats to their countries, after only climate change and pandemics. A broader survey in Spring 2018 that covered 26 countries showed a similar prevalence of fear of terrorism, specifically from the terrorist group known as the Islamic State of Iraq and Syria (ISIS), among populations in Europe, North America, Asia-Pacific, Africa and the Middle East (see Fig 1).

Climate change, ISIS and cyberattacks rank as top threats across North America, Europe, Asia-Pacific, the Middle East and Africa, but not in Latin America

___ is a major threat to our country

	Top threat	Global climate change	The Islamic militant group known as ISIS	Cyberattacks from other countries
		%	%	%
U.S.	Cyberattacks	59	62	**74**
Canada	Climate	**66**	54	57
France	ISIS	83	**87**	67
Germany	Climate	**71**	68	66
Greece	Climate	**90**	69	63
Hungary	Climate	**66**	59	35
Italy	ISIS	71	**80**	45
Netherlands	Cyberattacks	70	67	**72**
Poland	Russia	55	59	53
Spain	Climate	**81**	75	59
Sweden	Climate	**69**	61	55
UK	Climate	**66**	64	64
Russia	ISIS	43	**62**	36
Australia	Climate	**60**	59	58
Indonesia	ISIS	56	**81**	56
Japan	Cyberattacks	75	52	**81**
Philippines	ISIS	67	**79**	69
South Korea	Climate	**86**	63	81
Israel	ISIS	38	**47**	42
Tunisia	ISIS	61	**81**	65
Kenya	Climate	**71**	64	65
Nigeria	ISIS	41	**61**	47
South Africa	Cyberattacks	59	43	**61**
Argentina	Climate	**73**	53	58
Brazil	Climate	**72**	53	61
Mexico	Climate	**80**	34	60

Note: Bolded figures note the top concern in each country.
Underlined figures note the second-highest concern in each country.
Source: Spring 2018 Global Attitudes Survey.

PEW RESEARCH CENTER

Fig. 1. Pew Spring 2018 Global Attitudes Survey

Inspiring public confidence in the state's ability to deal with terrorism is clearly crucial. But how can a government say trust us to protect you from terrorism, when history provides ample evidence of failure? Indeed, al-Qaeda's 9/11 attacks on the United States in 2001, and the Christchurch mosque shootings in New

[1] Pew Research Center, *Despite Pandemic*.

Zealand in 2019 show governments can fail spectacularly in dealing with both ends of the spectrum: a terrorist group that had declared war on the West and left a long trail as it went about planning several simultaneous attacks using airplanes, and a lone right-wing extremist no one bothered to look at as he went about amassing firearms and choosing his targets because he did not fall into the usual suspect pool.[2] Among the government's deficiencies, the Commission of Inquiry set up by the New Zealand government to investigate the Christchurch attack noted, was not having "an overarching policy document describing its national approach to counter-terrorism", and not holding "planned and regular public engagement on the terrorism risks facing New Zealanders at home and abroad and measures taken to counter those risks".[3]

In the post-9/11 world, publicising national counter-terrorism policies as a strategic imperative appears to have become an important tool to reassure the public that their government is doing everything possible to protect them against terrorism, to signal a state's resolve to hunt down and punish those intent on killing and traumatising its citizens (see Fig. 2).

The US response to 9/11 was to declare a global war on terrorism and to send troops into Afghanistan to root out al-Qaeda. In February 2003, as the US prepared to invade Iraq in search of weapons of mass destruction, the Bush Administration codified its doctrine of pre-emption in a *National Strategy on Combatting Terrorism*[4] that revolved around 4Ds:

Defeat terrorists and their organisations
Deny sponsorship, support and sanctuary to terrorists
Diminish the underlying conditions that terrorists seek to exploit
Defend US citizens and interests at home and abroad

It meant, in President George W Bush's words, that the US would: "First, make no distinction between terrorists and the nations that harbor them — and hold both to account. Second, take the fight to the enemy overseas before they can attack us again here at home. Third, confront threats before they fully materialize. And fourth, advance liberty and hope as an alternative to the enemy's ideology of repression and fear."[5]

Obviously, not all nations subscribe to the unilateral use of pre-emptive strikes against an immediate or perceived terrorist threat abroad, nor do many have the wherewithal to do so. Most national security strategies describe more modest means of countering terrorism.

For example, Singapore, which in late 2001 foiled a planned wave of suicide bombings by al-Qaeda in partnership with a regional group called Jemaah Islamiyah, published a national security strategy in 2004 that described its *Fight Against Terror* as an "integrated, layered approach [that] is structured around the *Prevention*, *Protection* and *Response* domains." Under the heading "Why do we need this document", it described its goal as one of providing "all Singaporeans with a sense of where we are now, where we must go and what we must do in this security landscape."

---

2 See the reports of the *National Commission on Terrorist Attacks Upon the United States* (also known as the 9/11 Report), and the *Royal Commission of Inquiry into the terrorist attack on Christchurch mosques* on 15 March 2019 (also known as the Christchurch Report).

3 Royal Commission, *The Christchurch Report*.

4 This strategy was revised in 2006 and subsequent US presidents have issued their own national strategies that, while worded differently – Bush's global war on terror (GWOT) became countering violent extremism (CVE) under Obama – represent more continuity than change in the operationalisation of policy.

5 Bush, *Decision Points*.

In July 2006, one year after the 7/7 suicide bombings in London by four "homegrown extremists" who had pledged allegiance to al-Qaeda, the United Kingdom unveiled parts of a long-term strategy for countering international terrorism that it had developed in early 2003. Called CONTEST, the strategy aimed to reduce "the risk from international terrorism, so that people can go about their daily lives freely and with confidence" by following four Ps:

Prevent terrorism by tackling the radicalisation of individuals
Pursue terrorists and those that sponsor them
Protect the public, key national services, and UK interests overseas
Prepare for the consequences of a terrorist attack

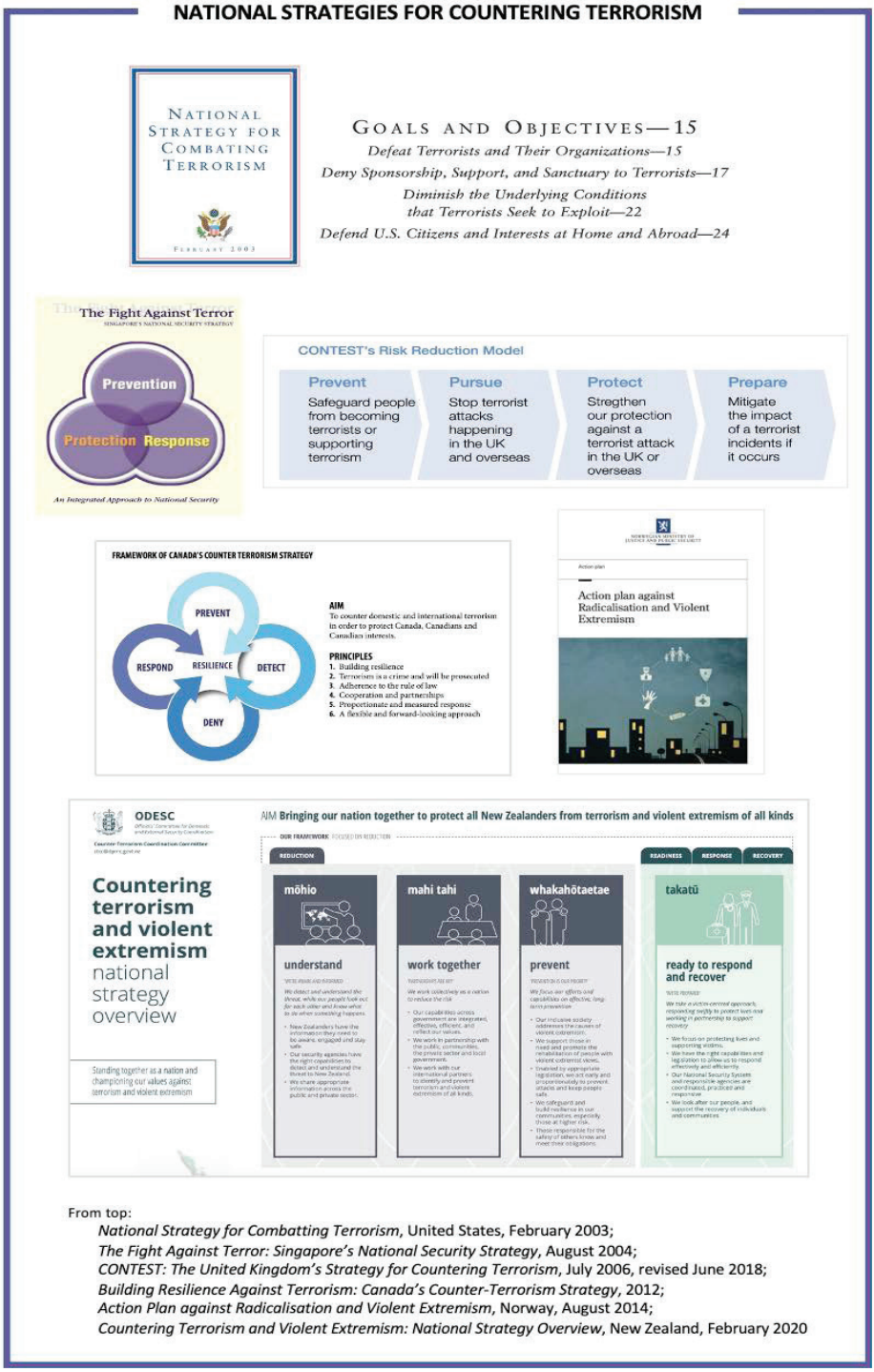
Following the massacre of 77 people on 22 July 2011 by a lone far-right extremist, Norway launched an *Action Plan against Radicalisation and Violent Extremism* in 2014. A multi-ministry effort, the plan was unveiled as "a framework for a targeted, strategic effort" in preventing recruitment to violent extremism. It called for more information, more cooperation and better coordination of efforts.

Six months after the Christchurch attack, the New Zealand Cabinet approved a high-level *Countering terrorism and violent extremism national strategy overview* in September 2019. The strategy document published in February 2020 promised 4Rs: *Reduction, Readiness, Response, Recovery*. Designed around a framework of reducing the risk of terrorism and being ready to respond to and recover from an attack, a key prong of this 4Rs strategy is to equip security agencies and the public with the capacity to detect and understand the terrorist threat so that everyone works collectively to reduce the risk, and knows what to do when an attack takes place.

Some states have also issued national strategy documents to press home the point that no country is immune from terrorism. Canada, which has faced the "full spectrum of terrorist threats", used its response to the long-delayed release of a Commission of Inquiry report on the 1985 bombing of Air India Flight 182 by Sikh extremists – the country's worst terrorist attack – to launch its *Building Resilience Against Terrorism* strategy in 2012. The Canadian document set out, for the first time, the government's *Prevent, Detect, Deny* and *Respond* strategy that is designed to provide a "flexible and forward-looking approach".

4Ps, 4Ds, 4Rs, some combination of Ps, Ds and Rs, or in the case of the Dutch national security strategy, a 5th P for *procure*, as in gather and assess in a timely manner intelligence about potential terrorist plots – these strategies invariably described legislation, policies and initiatives to ensure strategic convergence and operational coordination to deter and prevent terrorist attacks from happening at home. In the immediate post-9/11 years, there was a rush to harden potential targets and to increase the capacity of the intelligence, policing and security agencies to take coercive measures to interdict threats, to detain conspirators, and to respond quickly in the event of an attack.

The 7/7 attacks in London – and the growth of the homegrown terrorist – triggered a new policy trajectory: dealing with the challenges of radicalisation by violent extremist ideologies. Community outreach and building resilience became buzzwords in national strategy formulations, which now often take on the label of PCVE: preventing or countering violent extremism.



From top:
National Strategy for Combatting Terrorism, United States, February 2003;
The Fight Against Terror: Singapore's National Security Strategy, August 2004;
CONTEST: The United Kingdom's Strategy for Countering Terrorism, July 2006, revised June 2018;
Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy, 2012;
Action Plan against Radicalisation and Violent Extremism, Norway, August 2014;
Countering Terrorism and Violent Extremism: National Strategy Overview, New Zealand, February 2020

. Fig. 2. National Counter-Terrorism Strategy goals of various states

What, however, is the effect of publicising such national strategies? Does putting on record the government's resolve to fight terrorism in all its forms inspire public confidence in the state's capability to do so? Is it a best practice?

What inspires public confidence in a state's counter-terrorism efforts?

NATO defines terrorism as the "unlawful use or threatened use of force or violence, instilling *fear and terror*, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives (emphasis added)."

As psychological warfare par excellence, terrorism terrorises by making people believe they cannot control their exposure to a horrific death that is indiscriminate and can occur anytime. Might constantly reminding people of threats not magnify their sense of danger? Some terrorism experts argue against counter-terrorism messaging because the "laws of fear"[6] suggest that reminding people of the need to defend against terrorism makes them more insecure by reminding them of the presence of mortal threats they cannot avoid or protect themselves against, not unless they take extreme measures such as avoiding planes, trains and buses, houses of worship, beach promenades and street markets, hotels and any place that attracts crowds. In the US, for instance, a 2017 Gallup poll found a record-high 38 percent of adults less willing to attend large events, 46 percent less willing to travel overseas, 32 per cent less willing to fly on an airplane, and 26 percent less willing to go into skyscrapers because of concerns related to terrorism, which 60 per cent believed would hit the US in the next several weeks. As recently as October 2019, nearly half of Americans said they were very or somewhat worried that they or a family member would be a victim of a terrorist attack. This level of personal fear is above average, but below the record-high of 59% in early October 2001, a few weeks after 9/11.[7]

Yet, polls have always shown that Americans largely trust the US government to protect them from terrorism, with 70 per cent saying in 2017 that they had a great deal or fair amount of confidence in the authorities being able to do so.[8] As Gallup notes,

> Majorities of Americans over the years have expressed confidence in their government to protect its citizens against terrorism. However, the level of trust has varied and remains lower than it was in the years immediately after 9/11. While confidence in the government to protect against terrorism was high after the 9/11 attacks, the 2015 attack in San Bernardino had the opposite effect – confidence in federal protection declined to a record low [of 55 per cent].[9]

---

6 Sunstein, *Laws of Fear*.

7 Brenan, *Americans Equally Worried About Mass Shooting and Terrorism*.

8 Schmid (2017) has noted that while consulting opinion polls is the easiest and most straightforward way of measuring the level of support for government policies in the field of counter-terrorism, among other issues, it is "an under-utilised instrument of research on terrorism". He argues that while there may be methodological challenges in the way surveys are conducted, "public opinion polls are the second most important instrument for assessing popular support – surpassed only by official and honest election balloting – to assess the strength of endorsement for one or another social cause, political party, religious movement or armed group."

9 McCarthy, *Seven in 10 Trust U.S. Government to Protect Against Terrorism*.

The paradox is that while the US has not been hit by a terrorist attack anywhere near the catastrophic scale of 9/11 in the last 20 years, public confidence in the government's ability to combat terrorism has never been as high as the 88 per cent recorded in the weeks after the attacks, when the public rallied around its leaders. Confidence in the government's protection under Presidents Bush and Barack Obama ranged from 67 per cent to 82 per cent in post-9/11 polls until San Bernardino, when a terrorist shooting left 14 dead and shook public confidence. That December 2015 attack by a husband and wife team on a Christmas party at one of their employers, the San Bernardino County Department of Public Health, perhaps brought home to Americans that it is "impossible to stop every violent individual from picking up a gun and shooting." As Daniel Byman (2017) notes, "had the attackers not pledged loyalty to ISIS, law enforcement and the media might have described the attacks as workplace violence, not terrorism. Once officials attributed the acts to ISIS-linked terrorists, media attention – and thus the psychological impact – went through the roof. … [L]one wolves frighten people because they can strike anywhere. The 9/11 attacks targeted the symbols of U.S. financial, military, and political power; for many, the attacks struck at their identity as Americans but did not affect their personal security. A massacre at a nightclub or an office party, by contrast, hits much closer to home."[10]

Aaron M. Hoffman (2018) argues that people feel safer when they can see effective counterterrorism in action, when they are shown evidence that their government's counterterrorism policies work.[11] While colour-coded warning systems such as the one the US government deployed after the 9/11 attacks made people more nervous about terrorism, not more vigilant, television news reports about counterterrorism are associated with increases in public trust in government, opinion polls show. Militarised counterterrorism successes are especially effective; the US and NATO military campaigns to remove the Taliban from control of Afghanistan, and the subsequent killing of Osama bin Laden, produced the strongest results (see Fig. 3) because "people feel more secure when they believe that governments are degrading the capacity of terrorists to do harm to others".[12]

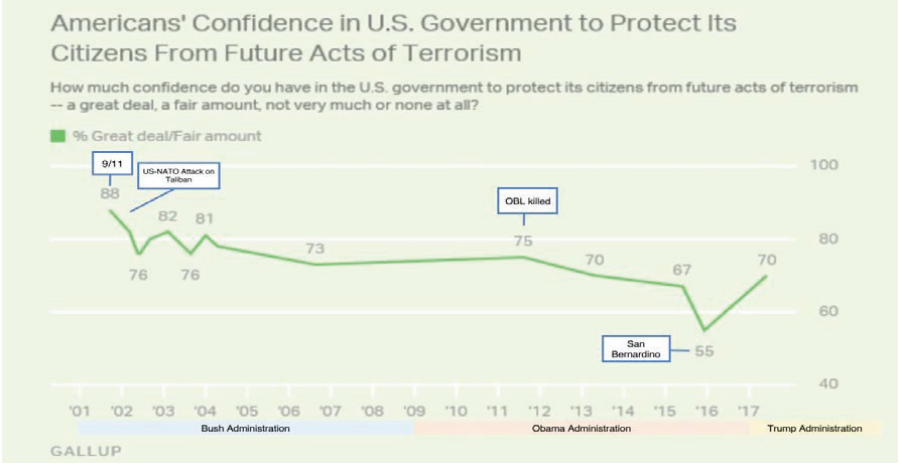


Fig. 3. Gallup Poll Results of US Public Confidence the Government Can Prevent Terrorism (2001-2017), with annotations by the author

[10] Byman, *How to hunt a lone wolf*.
[11] Hoffman, *People feel safer.*
[12] *Ibid*.

Criminal justice efforts have a similar effect of reassuring people about their safety[13], which is why governments regularly announce arrests of terrorist suspects and the foiling of terrorist conspiracies.

However, context is important, for a government that does not enjoy a basic level of trust of its citizens may not be able to reassure them. The March 11, 2004 bombing of four commuter trains in Madrid that killed 192 people and injured more than 2000, offers an instructive lesson. The then Spanish government blamed the Basque militant group ETA for the deadliest terrorist attack in Spain's history, and continued to do so even when there was strong evidence that al-Qaeda-inspired militants were behind the attacks. Many Spaniards believed the country was being "punished" for Spain's involvement in the US occupation of Iraq, which was extremely unpopular with the Spanish people but supported by the government. Public anger caused the ruling party to lose its majority at the polls four days after the bombings.[14] The new government in Madrid soon withdrew Spanish troops from the US-led coalition in Iraq, handing al-Qaeda a tactical victory in demonstrating that a well-timed terrorist attack can impact national elections and change policy in a democracy.

Manipulating the facts about a terrorist attack to suit political ends clearly do not work. What then are the right steps to build public confidence and mitigate fear of terrorism? There is currently not much research into the psychology of counter-terrorism, except perhaps in terms of strategic communications. Hoffman and Shelby (2017) make a passionate case for effective messaging of counter-terrorism policy:

> "The aim of terrorism," as Lenin explained, "is to terrify." Yet, governments focus on preventing the next attack by attending to material aspects of security: fortifying targets, increasing executive authority, recruiting first responders, and monitoring suspicious activity. Neutralizing terrorism's psychological effects is mostly an afterthought. … Ceding terrorism's psychological effects to perpetrators is an unjustified concession to attackers that perpetuates the illusion that terrorism works. The sense of insecurity terrorism engenders can be managed.[15]

"Not if an attack takes place, but when"

Governments are often faulted for lapses when an attack takes place. But is it really possible to prevent every attack? Can governments stay ahead of the curve when terrorist tactics are limited only by their imagination? As practitioners well know, policymaking is usually an incremental process, requiring political negotiations, buy-in from various stakeholders and funding from lawmakers. The patient policymaker keeps a few initiatives on the shelf, to be pulled out when a terrorist event at home or an audacious terrorist attack abroad creates a groundswell of public demand for action. For instance, in the immediate aftermath of 9/11,

[13] Hoffman and Shelby, *When the "Laws of Fear"*, 618–631.
[14] Burridge, *Spain remembers*.
[15] Hoffmann and Shelby, *When the "Laws of Fear"*.

governments in many countries set up ministerial-level steering committees and task forces to beef up the security and surveillance of commercial aviation and critical installations, border controls, and intelligence gathering and sharing.[16] In what then United Nations Secretary-General (UNSG) Kofi Annan called a moment of "moral clarity", the Security Council adopted a far-reaching resolution UNSCR 1373 (2001) that required Member States to cooperate in a wide range of areas, from suppressing the financing of terrorism, to providing early warning, cooperating in criminal investigations, and exchanging information on possible terrorist acts.[17]

Since then, countries have significantly altered their domestic counterterrorism programmes, laws, and institutions to cope with the evolving threat represented by al-Qaeda and its successors. As the European Union (EU) noted in a 2017 study for the European Parliament, its counter-terrorism agenda "has been to a large extent 'crisis-driven', and was heavily influenced by various major shocks: 9/11; the Madrid and London bombings; and the rise of the Islamic State in Iraq and Syria (ISIS) and; the terrorist attacks in France of 2015 and 2016; and the attacks in Brussels and Berlin in 2016."[18] This pattern of a crisis-driven counter-terrorism policy agenda can be seen not only among EU member states, but also across the globe.

In short, most counter-terrorism policies are designed to prevent the last major attack. This means that there will always be blind spots as countries have been focussing primarily on "Islamist terrorism" because the majority of the deadliest attacks since 9/11 have been in the name of al-Qaeda, ISIS, or their regional affiliates.

Recent large scale terrorist attacks by right wing extremists targeting minorities, in Christchurch, New Zealand (March 2019), El Paso, United States (August 2019), and in Germany – Halle (October 2019) and Hanau (February 2020) – have, however, raised questions as to whether governments are missing warning signs because they, and most terrorism researchers, are focusing so much of their attention on Islamist extremists, they have failed to understand the potential for violence from the far right, white supremacists and other ethno-nationalist extremists.

Indeed, the Christchurch Report concluded that "an inappropriate concentration of counter-terrorism resources on the threat of Islamist extremist terrorism" by the New Zealand government meant "there had been no substantial assessments of other potential threats of terrorism." The Report found, however, that the terrorist maintained such good operational security that his planning and preparation could not have been detected "except by chance". In other words, the authorities could not have prevented that attack because they never saw it coming, and luck was not on their side.

---

16 Rand Europe, *Quick scan.*
17 Annan, *Addressing Assembly.*
18 European Union, *The EU's Policies.*

And that is another reality that policymakers in some countries are acknowledging through their national strategy documents and political rhetoric: counter-terrorism policies are about risk management, not risk elimination, and the existential threat is not coming from abroad, but from within. For example, when the United Kingdom revised its national counter-terrorism strategy in 2018, it labelled its 4Ps response "a risk reduction model". Since ISIS turned the idea of a caliphate from aspirational to reality and incited followers everywhere – the lone wolves, released terrorist convicts and returned foreign fighters alike – to mount attacks using everyday tools such as cars and knifes, the mantra quietly adopted in many nations to prepare citizens has been: "Not if an attack takes place, but when."

Increasingly therefore, countering terrorism is taking on the form of preparing the public to survive an attack, and for society to bounce back stronger the day after. For the longer term threat from terrorism is to institutional and societal resilience. As UNSG António Guterres noted at the opening of the UN's Virtual Counter-Terrorism Week in July 2020, terrorist groups like "ISIL, Al-Qaida, their regional affiliates – as well as neo-Nazis, white supremacists and other hate groups – seek to *exploit divisions, local conflicts, governance failures and grievances* to advance their objectives (emphasis added)."[19] Not surprisingly, the UN chose "Building Institutional and Social Resilience to Terrorism" as the theme for its 2020 High-level Conference on Counter-Terrorism, until the conference itself was delayed by the more urgent threat of the COVID-19 pandemic.

Applying Best Practices to Counter-Terrorism Policymaking

The UN's Counter-Terrorism Executive Directorate (CTED), which has the job of conducting expert assessments of Member States' efforts to fulfil their obligations under various UN resolutions and conventions, identify short-falls, and recommend best practices, describes a best practice "as a technique, an activity, a strategy, a methodology or approach that has been shown, through application and evaluation, to be effective and/or efficient in achieving a desired result".[20]

For governments to get buy-in from stakeholders, being able to point to the effectiveness of counter-terrorism policy is not just an academic exercise, but an important political issue. The study of policy effectiveness is, however, plagued by both theoretical underdevelopment and a lack of methodological grounding.[21] Indeed, there are experts who believe that "a community of practice cannot reliably address the question which policy intervention or program deserve to be labelled as 'good' or 'best' practice" and with preventive counter-terrorism policy, the attribution problem is particularly acute because a successful attack does not necessarily mean a particular preventive policy has failed, and if no attacks take place, it is even more difficult to establish causality.[22]

[19] Guterres, *Remarks at the opening.*
[20] Millar *et.al. Report on Standards*.
[21] Van Um and Pisoiu, *Effective Counterterrorism*.
[22] Bossong, *Assessing the EU's Added Value*.

It does not help that national strategy documents may not be as salient as they used to be, particularly those issued in recent years. In late 2015, alarmed by the "barbaric crimes" of ISIS and Boko Haram, and the large numbers of foreign fighters drawn to Syria, then UNSG Ban Ki-Moon urged Member States to draw up national plans of action to prevent or counter violent extremism.[23] Thus began a new surge in the publication of national PCVE strategy documents, with various UN agencies providing substantive guidance on promising practices. But the similarity in language in many of these national strategies has also raised concerns that some governments are doing a copy and paste, more intent on ticking the suggested boxes than in ensuring they have a coherent, integrated and coordinated response that specifically addresses their domestic context. An independent review of several national PCVE strategies shows "certain measures are listed across strategies with a significant degree of regularity and consistency", although as authors Feve and Dewes (2019) note: "This is not necessarily problematic, and it is reasonable to expect that countries will source inspiration from each other and from a common body of international good practice."[24]

The problem, however, is that there is no one-size-fits-all model. If countries are not developing policies through a rigorous process that includes stakeholder consultation, risk assessment, evidence gathering, and policy synthesis, testing and calibration[25], are they adopting practices that meet their needs?

The complexities and limitations of evaluating the effectiveness of policy measures in counter-terrorism has led at least one NATO document to define best practices simply as "what works". A slightly more useful definition of best practice might be this: an approach or technique or activity or strategy

- that has been successfully implemented in at least one country (i.e. field tested),
- shown to achieve a desired result without causing further harm or damage,
- is superior to other methods, and
- is transferable elsewhere.

Almost all national, regional and international counter-terrorism strategies have a line about sharing best practices. But as terrorist groups are also learning organisations, countries sometimes classify highly effective practices that might lose their efficacy once publicised. At the same time, policy cannot in the face of a threat wait for perfect analysis. Recommendations for good or best practices thus have to be based on a survey of what has already been tried out and the known results as shared by practitioners. Ultimately, however, what is best practice has to be contextually mediated – what is optimal for a specific society?

---

[23] UNGA, *Plan of Action*.

[24] Feve and Dews, *National Strategies.*

[25] The UN Office of Counter-Terrorism, *Reference Guide* identifies procedural good practices and lessons learned in the development of strategies. Drawing from more established fields of policymaking such as development, peace-building, conflict resolution, and women, peace, and security, it recommends those involved in drafting strategies ask a series of questions clustered around six components: Establish, Gather, Analyse, Develop, Implement and Monitor. (For a useful summary see Feve and Dewes, *National Strategies*.)

When the EU conducted its first ever assessment of the national anti-terrorist arrangements of its Member States through a peer evaluation beginning 2003, it carefully identified *national good practices* with a significance for all or most other Member States as best practices to be offered as recommendations to close security gaps and enhance existing capacities from an operational and practical perspective. With the first review focused on national responsibilities at government ministry, security and intelligence service and law enforcement agency level, the final report also noted that each State was free to implement the recommended practices according to its *national legal and political framework*.[26]

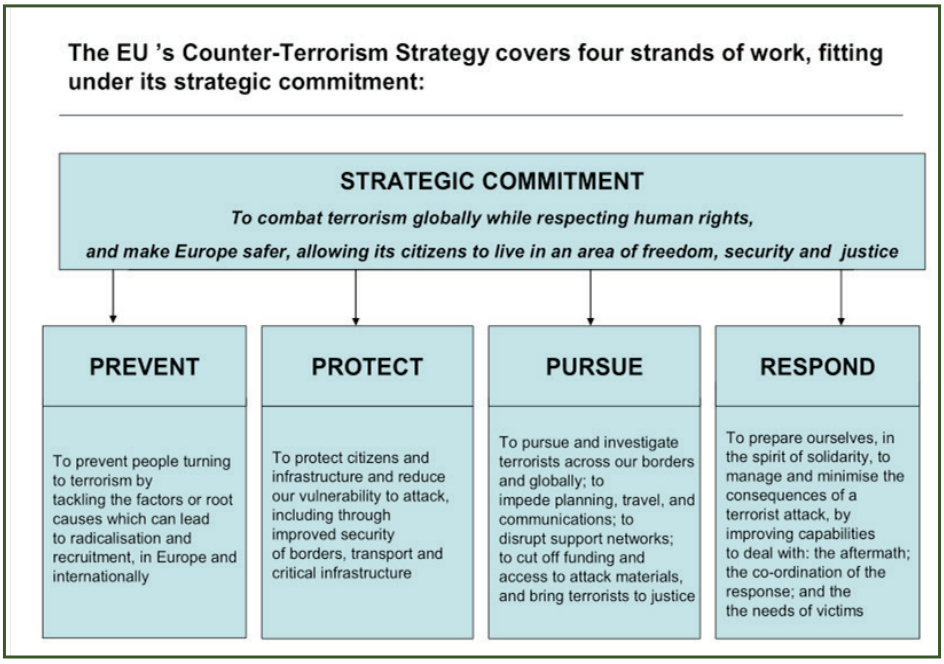


Fig. 4. Extract of the European Union Counter-Terrorism Strategy document submitted to the European Council on 30 November 2005

In 2005, the EU itself adopted a counter-terrorism strategy with a 3PR matrix (see Fig. 4) not unlike the UK's 4Ps template, which the UK had advocated during its EU presidency that year. The 3PR framework allows the EU to analyse the national strategies of Member States in a more systematic manner, and to offer guidelines on the specific resources required to counter the threat.

When it became obvious that the phenomenon of homegrown radicalisation was not going away, the EU adopted a strategy for combating radicalisation and recruitment to terrorism in 2008. More recently, in light of evolving trends precipitated by the rise of ISIS – lone-actor terrorism, foreign fighters, use of social media by terrorists – the EU revised this strategy and in December 2014, adopted an expanded set of guidelines for its implementation. Among the key points:

[26] Council of the European Union, *Final report.*

- Experiences from the past years have revealed that countering radicalisation and recruitment to terrorism effectively requires a balanced approach between security-related measures and efforts to tackle those factors that may create an environment conducive to radicalisation and recruitment to terrorism.
- The challenge will not be met by governments working alone, but by collaboration with communities, civil society, NGOs and the private sector. It requires a joint effort at local, regional, national, European and international level.

The good practices recommended include:

- Enhancing government communications to not just describe policy decisions and support their implementation clearly and consistently, but also to communicate what the EU stands for, its norms and values: international law, human rights and the rule of law,
- Challenging the terrorist narrative, especially online,
- Supporting and amplifying counter-narratives emanating from those with local influence,
- Training and equipping first line practitioners like teachers, social and health care workers, religious leaders, community police officers, and prison staff to provide them with a better understanding of radicalisation and recruitment to terrorism, and skills to discuss related issues,
- Supporting individuals and civil society to build resilience,
- Supporting disengagement initiatives,
- Supporting further research into the trends and challenges of radicalisation and recruitment.[27]

Is there a working model that includes most, if not all of these good practices? A non-EU country, Singapore, appears to have one.

The Singapore Model: Engaging the Whole of Society

Singapore maintains what the US State Department's 2019 Country Reports on Terrorism describes as "a 'not if, but when' stance regarding the likelihood of terrorist attacks within the city-state." The Singapore government describes its approach to countering terrorism as "multi-layered", made up of "hard rings of defence" formed by border security (with the borders pushed out through the strategic use of visa policies) and a protective infrastructure manned by the security agencies and the military, and "soft rings inside to cushion the possible impact of terrorism on our hearts and minds."[28] A key policy prong is community engagement.

As best practices go, community engagement has a long track record. It was used by the British in Northern Ireland, and after the 7/7 attacks in London, once again took "centre stage" as governments saw a need to "work in partnership with Muslim communities to prevent young people from being radicalised in the first place, and to ensure that communities were resilient enough to respond to, and challenge extremists from within."[29] Advocates of community engagement

[27] Council of the European Union, *Revised EU Strategy.*
[28] Latif, *Hearts of Resilience*.
[29] Briggs, *Community engagement*, 971-981.

believe that, as a principle, it has earned its place in national counter-terrorism policies. Certainly, it is cited in many national PCVE strategies. However, uneven implementation in countries in the West that emphasised outreach to Muslim communities as part of their community engagement and counterterrorism efforts has led to the practice being "accused of 'securitizing' relations between Muslims and the government, meaning that the government appears to interact with Muslims primarily through security organs to deal with security issues."[30]

The EU's 2014 *Revised Strategy for Combating Radicalisation and Recruitment to Terrorism* offers this helpful advice: "Community engagement should be broad-based and should reflect the diversity of the community." Only by involving a wider range of civil society and the private sector, it suggests, can governments draw on the tools and resources and the insights they have to offer.

However, in the age of the homegrown extremist and the lone wolf terrorist, whether of the left-wing, right-wing, or religious variety, there is no escaping the fact that governments need all the help they can get from their own citizens to prevent attacks. As the key architect of Singapore's post-9/11 counter-terrorism policy, Benny Lim, puts it:

> The quality of community engagement reflects not just societal support for the government's counter-terrorism security action, but also enables the whole of society to be a partner in rejecting terrorist narratives and extremist ideologies and be a vital ground resource for early warning and intelligence. The challenge is that such counter-terrorism community engagement involves a dynamic composite of both Muslim and non-Muslim constituencies and their often diverse religious elites at the same time – not always easy to do but needs to be done. And in the context of legacy issues, this is probably more difficult in some countries than others.[31]

Singapore's community engagement programme has gone through various iterations. A multicultural country with a population of 5.7 million people, of which slightly more than 4 million are citizens and permanent residents of various races and ethnicities, and 1.65 million are expatriates of various nationalities, it is also a secular state that gives space for different religions to celebrate their diversity. The Chinese majority and the Malay, Indian and Eurasian minorities are encouraged to negotiate their differences while celebrating commonalities. This has been reinforced by a common education curriculum that emphasises national identity and values while supporting parish schools and madrassahs to teach religious knowledge and prayer. Civic society is also encouraged to work towards increasing understanding of different beliefs and cultures. Yet after more than 50 years of nation-building, the government remains concerned that this hard-won racial and religious harmony, tested in the past by race riots and underpinned now by legislation mandating separation of state and religion (in other words, no religious meddling in politics), can be sundered by a terrorist attack perpetrated in the name of race or religion.

In the fight against terrorism, Singapore is no different from many states in being somewhat crisis-driven in its approach. The key difference is that its community outreach is led by the

[30] Fishman and Lebovich, *Countering Domestic Radicalization.*

[31] Author interview with Benny Lim, November 19, 2020. Lim was Director of the Internal Security Department from 1997 to 2004, Permanent Secretary for Home Affairs from 2004 to 2011, and Permanent Secretary for National Security and Intelligence Coordination from 2011 to 2016, when he retired from public service.

highest level of political office – the Prime Minister (PM) himself. When Singapore's Internal Security Department (ISD) uncovered in late 2001 an al-Qaeda plot to conduct six suicide truck bombings in Singapore that had been proposed and planned for by the Singapore cell of a regional terrorist group called Jemaah Islamiyah (JI), the island-state's political leadership decided it had to embrace the local Muslim community as a major stakeholder in fighting terrorism if Singapore's carefully calibrated religious harmony were to hold. Accordingly, ISD officers visited and reached out to Muslim organisations and leaders even before the details of the JI-al-Qaeda plot were made public, which included the fact that the Singapore members all professed to be fighting for an Islamic state and some had trained with al-Qaeda in Afghanistan and others with regional militant groups in Mindanao. With the PM in attendance, ISD officers also twice briefed an audience of over 1,700 grassroots leaders.[32]

Quietly, ISD also invited prominent religious cler ics to help it rehabilitate the terrorist suspects, who had been arrested under Singapore's preventive detention law, the Internal Security Act (ISA). Even as ISD rounded up suspects, it knew it had to plan for their eventual release, since the ISA is designed to be used to neutralise threats to national security and detention orders are for a maximum of two years in the first instance. The government decided it was "not appropriate" to try radicalised individuals or extremists in open court, as doing so "could make things worse" and inadvertently reveal intelligence operations,[33] opting instead for "a clear process – detain, rehabilitate and release".[34]

Although initially apprehensive as to how their involvement might be perceived, several Islamic clerics stepped forward to work with ISD to craft the rehabilitation approach. Volunteers who act in their personal capacities, not for any group, they receive no government salaries or stipends, only lessons in counselling skills. Now widely known and lauded as the Religious Rehabilitation Group (RRG), the clerics counsel not only detainees but also individuals at-risk in the community,[35] working alongside but separately from government psychologists who counsel the detainees on social coping and recommend vocational training for their social reintegration. Another groups of volunteers, who call themselves the Aftercare Group, looks after families and children of detainees. The early involvement of these two community groups was also crucial on a strategic level because it enabled Muslim Singaporeans to see themselves not as a community under siege, but as a crucial partner of the secular state in ensuring national security. This partnership between the community and the security authorities in Singapore has been possible largely because ISD officers began building relationships of trust with key community leaders long before 9/11. Soon after the 9/11 attacks, a member of the Muslim community in Singapore informed ISD that an acquaintance of his had boasted

---

32 Sim, *Lessons from the Singapore.*

33 Under the Internal Security Act, a detention order must be reviewed by an independent ISA advisory board headed by a Supreme Court judge that hears directly from the accused, who has the right to counsel of his own choice and who may question ISD officers and witnesses under oath. The hearing is, however, held *in camera*.

34 Hussain, *ISIS bride.*

35 For a short description of Singapore's deradicalisation approach and the lessons it offers other countries like the United Kingdom that is rethinking its approach to managing terrorism offenders, see Jayakumar and Pantucci (2020). They have calculated that of the first wave of JI cases detained in Singapore post-9/11, around 90% were eventually released following assessments by RRG clerics and psychologists from the Home Affairs Ministry that they had changed their perspective on the use of violence. The remaining 10% (fewer than 10 individuals) were key influencers, or hardened radicals whose ideas are unlikely to change, and remain incarcerated, with the RRG and government psychologists continuing to engage with them.

that he personally knew al-Qaeda leader Osama bin Laden. That tip-off eventually led to the uncovering of JI and the foiling of the al-Qaeda plot in Singapore.[36]

The PM remained concerned, however, that the close-call "threatened to sow fear and mistrust among our different races". And so apart from upgrading the security forces and deepening international cooperation on terrorism issues, the government "identified the critical need to maintain strong and enduring community ties … to engage community leaders to calm the ground, and get Singaporeans to see the threat for what it was – acts by misguided extremist individuals and not a threat posed by Islam or Muslims in general."[37]

Thus was born Singapore's Community Engagement Programme (CEP), which began in earnest after the London 7/7 attacks made clear the threat posed by homegrown terrorists, and the resulting rise in hate crimes against Muslims across the Western world. The CEP comprised five clusters that covered the traditional grassroots leaders already active in the community; the tripartite group of businesses, unions and government; schools where parents and students of different races interact; clans and associations including religious groups; and the media and academics, especially those studying terrorism issues. Top-down in conception, the CEP was "bottom-up in terms of actual interpretation on the ground", says Benny Lim, as the government saw its job as being to "manage and coordinate diversity of domains without displacing their sense of ownership."[38] The true test of the CEP's effectiveness would, obviously, only be apparent in the event of an attack, in how Singaporeans held together and returned to normalcy. But with each year passing without incident, sustaining public interest became challenging.

In 2016, the government put the CEP on steroids, revitalising it as SGSecure, a national counter-terrorism programme "to sensitise, train and mobilise the community to play a part to prevent and deal with a terrorist attack." The impetus was the increasing number of Singaporeans radicalised online by ISIS propaganda and seeking to travel to Syria to join the group, or to stage attacks at home if stopped from going.

Reminding Singaporeans that the nature of terrorist attacks has changed to include self-radicalised lone wolves who could attack them at "the MRT station near your home … your favourite hawker centres or shopping malls … anywhere", using "ordinary objects such as knives, parangs and trucks", PM Lee Hsien Loong issued a call to action at the official launch of SGSecure in September 2016, adding:

> Terrorism threats are not going to disappear for quite a long time and we must expect the terrorists to continue to attack and to plan to attack Singapore. They are targeting not just our physical safety, but the fabric of our society. When we are confronted with something like this, we can respond in two ways. Either with fear, cowed, hankered down, pretend nothing is happening, pretend that the threats do not exist, and hope that the troubles will pass us by. Or we can stand up, look the problem straight in the face, understand the dangers we face, know what we can do, do what we can, now and continuing into the future, and make sure that if something does happen, we are ready.[39]

---

36 Sim, *Lessons from the Singapore.*

37 Latif, *Hearts of Resilience*.

38 *Ibid*.

39 Loong, *PM Lee Hsien Loong*.

Fig. 5. An early SGSecure poster downloaded from a dedicated website; www.sgsecure.gov.sg

SGSecure: Training and Mobilising the Community

To convince every Singaporean that they must assume some self-responsibility for protection against risk, for good relations between communities, and that all must do their part to shore up societal and national resilience, SGSecure offers them three roles:

- A Prepared Citizen, able to protect themselves and their families by learning to recognise signs of suspicious behaviour and suspicious items, and to report such activity to the police.
- An Active Responder, trained to react, to help others in times of emergency by administering life-saving skills such as cardiopulmonary resuscitation (CPR), or using an automated external defribillator (AED) in case somebody has a cardiac arrest.
- An Effective Mobiliser, a leader of the SGSecure movement who will champion its initiatives, resolving frictions that can undermine racial or religious harmony, in peacetime and during crises. A Mobiliser may be a religious leader, a grassroots activist, a unionist, a Home Team officer or Home Team volunteer[40], who has their own networks, and will work closely with Prepared Citizens, Responders, and other Mobilisers to develop crisis contingency plans for their networks and communities.

For organisations, there is an SGSecure@Workplaces programme to equip them with the knowledge and capabilities to deal with terror attacks, including guidance on preparing contingency response plans for different attack scenarios. Regular exercises simulating terrorist attacks are conducted in shopping malls and communal areas to test these plans.

To extend the outreach to as many people as possible in as short a time as possible, the government also developed an SGSecure app to be downloaded on smartphones to allow the public to receive alerts from the police in the event of an emergency and to make 999 calls

[40] The 10 law enforcement, internal security and domestic safety agencies that report to the Minister of Home Affairs are collectively known as the Home Team, whose common mission is to keep Singapore safe and secure. Most of these agencies have longstanding community engagement programmes that involve volunteers in activities such as crime prevention, preventive drug education, rehabilitation and re-integration of ex-offenders, fire safety and curbing problem gambling.

or send text messages to alert the police. The app also contains cheat sheets on behavioural changes that might be signs of radicalisation in a friend or loved one, tips on how to describe suspicious parcels, cars or individuals to the police, advice on what to do if caught in an attack (Run, Hide, Tell), quick lessons on improvised first aid techniques, and guidance for companies on how to protect their workplaces against different types of attacks such as an active shooter, car bombing or release of harmful chemicals.

In short, SGSecure is about teaching people how to survive an attack. And how to cope with the day after, the key tenets of which are "keep calm, do not spread rumours, care for others" (see Fig. 6).

Fig. 6. SGSecure poster for the day after

Is this whole-of-society approach to building a national consensus on fighting violent extremism and terrorism effective? A public perception survey the Singapore government conducted two years after launching SGSecure, in 2018, suggests it is meeting its goals, as Fig. 7 shows:

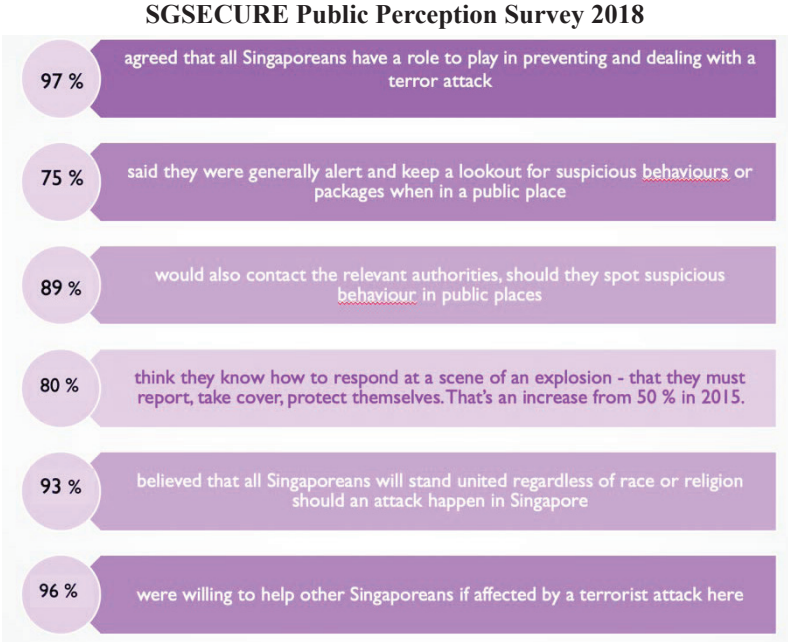
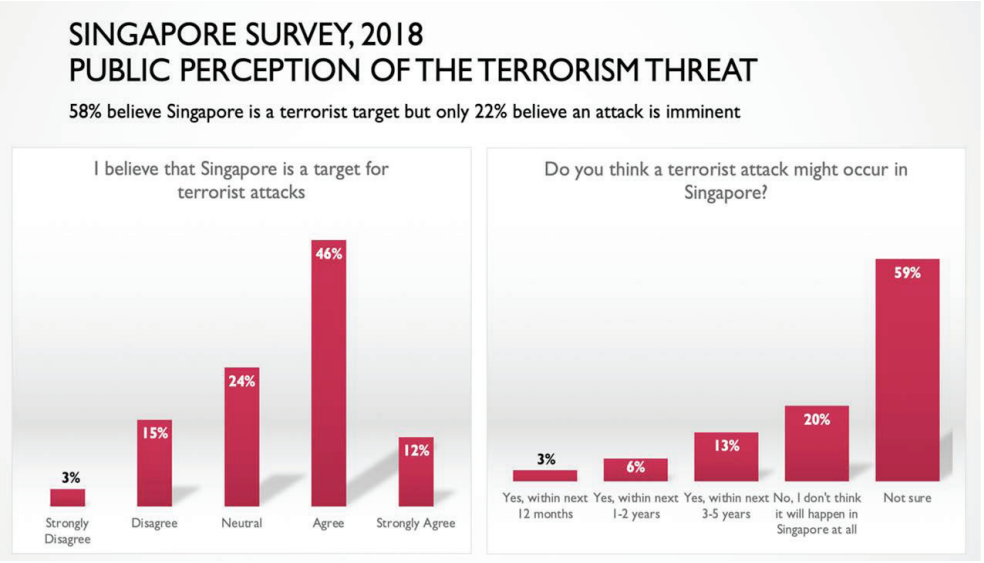


Fig. 7. Key Results of Public Perception Survey in Singapore in June -July 2018 to gauge perception of the terrorism threat, and public sentiments towards and participation in the SGSecure movement. The survey sample was representative of the national population, with a total of 2,010 Singapore Citizens and Permanent Residents aged 15 years and above interviewed face to face. (Data courtesy of Ministry of Home Affairs.)

Importantly, the survey results suggest that Singapore now has an informed and aware public that does not live in fear of terrorism despite constant reminders to remain vigilant. While close to 60% believe that Singapore is a target for terrorist groups, only 22% fear an attack might take place within 1-5 years.



Fig, 8. Public Perception Survey in Singapore conducted in June -July 2018 with 2,010 respondents (Singapore Citizens and Permanent Residents aged 15 years and above interviewed face to face). (Data courtesy of Ministry of Home Affairs.)

Confidence in the Singapore government's counter-terrorism capability also appears to be very high, with 85% of respondents saying they believe Singapore as a nation will be able to deal with a terrorist attack if it were to happen in Singapore today. Overall, Singaporeans give the government high points for preparedness and their own resilience in the face of a terrorist attack (see Fig. 9).

To keep up the momentum, the government regularly publicises cases of how Singaporeans have used the life-saving skills they learned, such as CPR and use of an AED, to save people in their neighbourhoods while waiting for paramedics to arrive. Some of the stories have been turned into short films that can be downloaded on the www.sgsecure.gov.sg website. Accordingly, the movement's tagline is now:

Our response matters, we make SGSecure.

Fig, 9. Public Perception Survey in Singapore conducted in June -July 2018 with 2,010 Singapore Citizens and Permanent Residents aged 15 years and above. (Data courtesy of Ministry of Home Affairs.)

But Can the Model be Transferred?

A key test of whether a model, approach or policy is a best practice is whether it is transferrable elsewhere. Singapore's counter-terrorism policy employs well-known best practices: preventing and pre-empting terrorism through the whole-of-government troika of good intelligence, effective law enforcement, and international cooperation, as well as a whole-of-society approach to train and mobilise a wide array of community groups to counter recruitment to violent extremist ideologies without stigmatising any particular religion or race. Top-down or bottom-up in conception and implementation, it is playing the long game, prepared to invest "time, energies and faith" in its SGSecure movement because it believes, says Benny Lim, that "social resilience, in terms of inter-communal peace and social cohesion when faced with the strains and tensions arising from a terrorist event, is the most important product of a successful and effective community engagement programme."[41]

Such community engagement programmes are usually difficult to start and often even more difficult to sustain over time. But it is also easier in some societies than in others because in the age of al-Qaeda and ISIS, it involves much negotiation between different religious communities and their elites. Singapore, for instance, practises what Ramakrishna calls a policy of "muscular secularism"[42] in that the state itself does not profess a state religion or promote any particular faith at the expense of others, but rather "acts as a neutral umpire between the contending interests of the various faiths." The state also actively seeks to "preserve and expand the Common Space shared by Singaporeans of all racial and religious backgrounds", discouraging exclusivist practices where people only interact with others of the same faith or exclude people of other faiths.

Elected political leaders also constantly remind Singaporeans that "the right to speak freely goes with the duty to act responsibly …. free speech for us stops at the boundary of giving offence to religion."[43] Unlike the French concept of secularism – *laicite* – the Singapore practice of secularism is interventionist, guaranteeing not only freedom of religion, the right of every person to practise his or her religious beliefs, but also protection "from any threats, hate speech or violence", Singapore Home Affairs Minister Shanmugam said in a speech at the RRG's annual seminar in November 2020. Amidst a global controversy over French President Emmanuel Macron's speech defending the right in France to publish the Charlie Hebdo cartoons, he promised that "the Charlie Hebdo types of cartoons will not be allowed in Singapore, whether they are about Catholicism or Protestants or Islam or Hindus."

In considering if a best practice is optimal for a country, it bears repeating that context is very important. The Singapore state considers any threat to its multi-racial and multi-religious fabric to be existential. Having studied how terrorist attacks like 9/11 and 7/7 led to hate crimes against Muslims, the Singapore government is convinced an attack on the city-state will have severe ramifications for communal relations that could lead to other types of

41 Author interview with Lim, November 19, 2020.
42 Ramakrishna, *Diagnosing "extremism,"* 26-47.
43 Shanmugam, *Speech by Minister for Home Affairs.*

violence. It is accordingly betting that it can prepare its people to survive a terrorist attack by demonstrating that the state is prepared to deal decisively with such acts and thus counter fears of terrorism.

In the final analysis, however, the transferability of good practices is about political will to take ownership of the problem and its solutions, clarity of goals, and fairness in implementation. Best practices are not panaceas. They are about principles applied to good practical ideas.

Bibliography

Annan, Kofi, (2001), "Secretary-General, Addressing Assembly on Terrorism, Calls for 'Immediate, Far-Reaching Changes' in UN Response to Terror", United Nations Press Release SG/SM/7977-GA9920, 01 October 2001, https://digitallibrary.un.org/record/449890 (Accessed 15 December 2020)

Bossong, Raphael, (2012), "Assessing the EU's Added Value in the Area of Terrorism Prevention and Violent Radicalisation", *Deutsches Institut für Wirtschaftsforschung (DIW)*, Economics of Security Working Paper No. 60, 2012.

Brenan, Megan, (2019), "Americans Equally Worried About Mass Shooting and Terrorism", *Gallup*, 11 October 2019, https://news.gallup.com/poll/267383/americans-equally-worried-mass-shooting-terrorism.aspx. (Accessed 15 December 2020)

Briggs, Rachel, (2010), "Community engagement for counterterrorism: lessons from the United Kingdom", *International Affairs*, July 2010 , Vol. 86, No. 4 (July 2010), pp. 971-981.

Burridge, Tom, (2014), "Spain remembers Madrid train bombings 10 years on", *BBC*, 11 March 2014, https://www.bbc.com/news/world-europe-26526704 (Accessed 15 December 2020)

Bush, George W., (2010), *Decision Points*, (New York: Crown Publishers).

Byman, Daniel, (2017), "How to hunt a lone wolf: Countering terrorists who act on their own", *Foreign Affairs* March/April 2017.

Council of the European Union, (2005), "Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism", Report 12168/3/05 REV 3, November 2005.

Council of the European Union, (2014), "Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism" Report 9956/14, 19 May 2014.

European Union, (2017), "The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness", European Parliament Policy Department for Citizens' Rights and Constitutional Affairs.

Feve, Sebastien, and David Dews, (2019), "National Strategies to Prevent and Counter Violent Extremism: An Independent Review", *Global Center on Cooperative Security*.

Fishman, Brian, and Andrew Lebovich, (2011), *Countering Domestic Radicalization: Lessons for Intelligence Collection and Community Outreach*, New America Foundation, June 2011.

Guterres, António, (2020), "Remarks at the opening of the Virtual Counter-Terrorism Week United Nations", UN Secretary-General, UN Headquarters, 06 July 2020, https://www.un.org/sg/en/content/sg/speeches/2020-07-06/remarks-opening-of-virtual-counter-terrorism-week-united-nations (Accessed 15 December 2020)

Hoffman, Aaron M., (2018), "People feel safer when they see effective counterterrorism policies in action", *LSE US Centre*, 30 July 2018, https://blogs.lse.ac.uk/usappblog/2018/07/30/people-feel-safer-when-they-see-effective-counterterrorism-polices-in-action/ (Accessed 15 December 2020)

Hoffman, Aaron M, and William Shelby, (2017), "When the "Laws of Fear" Do Not Apply: Effective Counterterrorism and the Sense of Security from Terrorism", *Political Research Quarterly*, Vol. 70, No. 3, pp. 618–631.

Hussain, Zakir, (2019), "ISIS bride and a fighter from Singapore said to have died in Syria, Terror threat remains a key concern, says Shanmugam, stressing need to be alert", *The Straits Times*, 04 Augusut 2019, https://www.straitstimes.com/singapore/isis-bride-and-a-fighter-from-spore-said-to-have-died-in-syria (Accessed 15 December 2020)

Jayakumar, Shashi and Raffaello Pantucci (2020). "The Singapore Model: A New Deradicalisation Approach for the UK?", *RUSI Newsbrief* , Vol. 40, No. 2.

Latif, Asad, (2011), *Hearts of Resilience: Singapore's Community Engagement Programme*, (Singapore: Institute of Southeast Asian Studies).

Loong, Lee Hsien, (2016), "PM Lee Hsien Loong at Official Launch of SGSecure", Prime Minister's Office, 24 September 2016, https://www.pmo.gov.sg/Newsroom/pm-lee-hsien-loong-official-launch-sgsecure (Accessed 15 December 2020)

McCarthy, Justin, (2017), "Seven in 10 Trust U.S. Government to Protect Against Terrorism", *Gallup*, 19 June 2017, https://news.gallup.com/poll/212558/seven-trust-government-protect-against-terrorism.aspx. (Accessed 15 December 2020)

Millar, Alistair, Jason Ipe, David Cortright, George A. Lopez, Anne Marbarger and Kathryn Lawall, (2006), "Report on Standards and Best Practices for Improving States' Implementation of UN Security Council Counter-Terrorism Mandates", *Global Center on Cooperative Security*, https://www.globalcenter.org/publications/report-on-standards-and-best-practices-for-improving-states-implementation-of-un-security-council-counter-terrorism-mandates/ (Accessed 15 December 2020)

Pew Research Center, (2020), "Despite Pandemic, Many Europeans Still See Climate Change as Greatest Threat to Their Countries", 09 September 2020, https://www.pewresearch.org/global/2020/09/09/despite-pandemic-many-europeans-still-see-climate-change-as-greatest-threat-to-their-countries/ (Accessed 15 December 2020)

Ramakrishna, Kumar, (2019), "Diagnosing "extremism": the case of "Muscular" Secularism in Singapore", *Behavioral Sciences of Terrorism and Political Aggression*, Vol. 11, No. 1, pp. 26-47.

RAND Database of Worldwide Terrorism Incidents, (1968 – 2009), https://www.rand.org/nsrd/projects/terrorism-incidents.html (Accessed 15 December 2020)

RAND Europe, (2002), "Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries", www.rand.org/pubs/monograph_reports/MR1590.html (accessed 15 December 2020)

Royal Commission of Inquiry into the terrorist attack on Christchurch mosques on 15 March 2019, (2020), "The Christchurch Report", 08 December 2020, https://christchurchattack.royalcommission.nz/the-report/ (Accessed 15 December 2020)

Schmid, Alex P., (2017), *Public Opinion Survey Data to Measure Sympathy and Support for Islamist Terrorism: A Look at Muslim Opinions on Al Qaeda and IS*, (The Hague: International Centre for Counter-Terrorism (ICCT))

Shanmugam, K., (2020), Speech by Minister for Home Affairs and Minister for Law at the 16th Religious Rehabilitation Group (RRG) Seminar, 24 November 2020, https://www.mha.gov.sg/newsroom/speeches/news/16th-religious-rehabilitation-group-seminar-speech-by-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law (Accessed 15 December 2020)

Sim, Susan, (2014), "Lessons from the Singapore Home Team Approach to Homefront Security" in James Forest, Russell Howard, Joanne Moore (eds.), *Homeland Security and Terrorism: Readings and Interpretations*, (Second Edition), (New York: McGraw-Hill).

Sunstein, Cass R., (2005), *Laws of Fear: Beyond the Precautionary Principle*, (Cambridge: Cambridge University Press).

United Nations General Assembly (UNGA), (2006), "Resolution adopted by the General Assembly on 8 September 2006: The United Nations Global Counter-Terrorism Strategy", Report A/RES/60/288, 20 September 2006.

United Nations General Assembly (UNGA), (2015), "Plan of Action to Prevent Violent Extremism: Report of the Secretary-General" A/70/674, 24 December 2015.

United Nations Office of Counter-Terrorism (UNOCT). (n.d.). *Reference Guide: Developing National and Regional Action Plans to Prevent Violent Extremism*.

Van Um, Eric, and Daniela Pisoiu, (2011), "Effective Counterterrorism: What Have We Learned so Far?", *Deutsches Institut für Wirtschaftsforschung (DIW)*, Economics of Security Working Paper No. 55.

CHAPTER IV

AN ORDER OF CYBER SECURITY MATURITY: PROTECTING CYBER DOMAINS FROM TERRORISM

Salih Bicakci

"The world is never going to be perfect, either on- or offline; so let's not set impossibly high standards for online."
Esther Dyson[1]

Terrorism and Cyberspace have a particular relationship. Cyberspace presents *sui generis* characteristics which affect related domains such as the kinetic world that we interact in, while terrorism has a polymorphic and liquid characteristic. As Hoffman (2006) has noted, it is arguably easier to define what makes as an act of terrorism with reference to acts of terrorism in history. But contemporary terrorists benefit from and take advantage of all the advantages of technology to achieve their goals. This situation obfuscates demarcation between terrorism and cyber domains. Countering terrorism in cyber domains requires a remarkable amount of effort.

This research is designed to assist cyber security staff in different sectors with examples of good practices in the field. However, the appearance of terrorism in cyber domain is distinctly different from other domains in the physical world and, as a result, presenting a one-fits-all model is certainly difficult for information and communication technologies. The author's approach has, therefore, been to compile extensively trialed practices within a general risk-based approach to mature the security and protection policies for computers, networks and relevant structures.

In the last decade, with the increase of digitalization, most of the services of private sector and state entities have been transferred across to the cyber domain. The digitalization process has also promoted the usage of new platforms and devices which have advanced the connectivity of people and services to each other. This hyperconnectedness has also produced new capabilities and opportunities for individuals, corporations and states. This shift has also connected the local with the global space. So, a node in hyperconnected cyberspace could easily reach the global level with an attack, a news story or simply an activity (such as a funny meme). This presents a unique opportunity for terrorist groups as they could achieve an extensive impact with minor investment. Cyber space, in this sense, presents an amplifying effect on terrorist attacks or actions.

[1] Anderson, *Security Engineering.*

Nature of Cyber Space

Cyberspace presents *sui generis* characteristics which we do not experience in the physical world. This new space is different to the other spaces experienced. Major problems that most of our organizations are built to respond to and interact with in the kinetic world do not exist in cyberspace. However, the power of cyberspace comes from its effects on the physical world. This is so substantial a change in the nature of the system that it is pushing the limits of conventional reactions and structures that are in place.

Dunn-Cavelty concisely defines cyberspace as an ecosystem and continues, "ecosystems are habitats for a variety of different species that co-exist, influence each other, and are affected by a variety of external forces. From this point of view, social and technological forces are symbiotic.[2]"

The symbiosis and the resulting effects of multiple actors interacting among several forces brings forth the concept of complex adaptive systems. Cyberspace is a complex adaptive system which has its *sui generis* characteristics. To comprehend its functionality is essential to build resilient organizations which can function effectively in this realm.

Choucri summarizes the properties of cyber space in seven articles[3]:

Temporality, "in the sense that chronological time is replaced by near instantaneity in the realization of action and in the potential reaction." In conventional structures, the functionality of the public or private organization is designed for multiple time zones. However, cyber threats are overriding these conventions and accepted realities by pushing the organizations to be operational 24/7.

Physicality, "meaning that activities undertaken or decisions made are not constrained by geography, spatial consideration, or sovereign boundaries." In cyber space, it is hard to determine precise origins. As a result, one of the major uncertainties in cyberspace is the origin of an attack. The principle human approach would be to try to find out the origin of attack and to fit it into a pattern that is consistent with the political situation. But we now have to adapt our organizations to understand that each attack could be independent from others without any geographical linkages. Additionally, simultaneous attacks could hit a target from multiple geographic locations, which is frequently observed in 'Bot' attacks. These types of attacks are also stretching the limits of organizations' capabilities. If there is no cognitive and institutional preparation for these types of attacks, organizations will have hectic times when trying to deal with the problem.

Permeation, "which refers to communication and activities that penetrate state boundaries and sovereign jurisdictions." Cyberspace and its capabilities are superseding the authorities of states. As a result, several states now plan to control cyberspace with various levels of regulations and by creating control points in both the hardware and the software. Conversely, there are tools and software on the market which defend freedoms and the rights of the individuals to overcome exactly those regulations of the states.

---

2 Cavelty, *From cyber-bombs*, 105-122.

3 Choucri, *Emerging Trends.*

Fluidity, "which refers to the ease with which shifts in patterns of interactions take place, with attendant configurations and reconfigurations, and emergence of new actors and modalities of interaction." The quick changing nature of cyberspace is introducing new actors and behaviors each day. This flexibility and fluidity makes it hard to construct concepts and long-lasting strategies.

Participation, **"**in the sense that access to cyber venues has already shown how barriers to activism and political expression can be reduced, and the wide range of effects that could then occur." In addition to political expression, there is a great deal of flexibility in the representation of ideas in cyberspace. The cyber domain permits users to present themselves with imagined identities or to remain completely anonymous. This false sense of freedom sense frequently promotes appearance of a disinhibiting effect[4].

Attribution, "where the basic property of cyberspace in this connection refers to the obscurity of identify for actors as well as linkages of actors to specific actions." In cyber space, attacks form the major part of the conflict. To connect any cyber attack to a perpetrator is a very significant challenge. Bots, spoofing IP, Proxies, VPNs and public wireless access points are some of the ways hackers or crackers hide their identity. A long and effortful process is required to clearly identify perpetrators. In the physical world, you can see the attacker and make your decision on how to deal with the attack based on the capacity of the attacker. However, in cyber space attribution is only a clue about the capacity of the attacker. The attacker could be a member of a state organization, or an organized crime group or a lone wolf. By assessing the breach or attack, you then have to decide how to proceed based on this limited information.

During a period of reduced sensations in the physical world, our brain is wired to use all our senses to protect us from any threat. A facial expression, the sound of footsteps in a dark street, less illuminated back streets or a smell would be a clue for us to understand a possible danger. However, in cyberspace you have limited usage of these sensors. In a video gaming platform or video conferencing you could experience some data from your sensors but these are not comparable to physical world experiences. In cybersecurity, the limited sensory experience really affects incident perceptions and the identification of preliminary signals.

As a state of altered perception, cyberspace has its own reality that mimics a state of consciousness akin to a dream. Reduced sensations and altered perceptions affect our cognitive capacities such as judgment and decision-making. In recent years, neurophysiology studies have shown that regular and continuous exposure to the altered perception of cyberspace could also change brain plasticity[5].

All these properties demonstrate how the dynamics of cyberspace are distinctly different from other domains and require special approaches to construct defensive tactics.

---

[4] Online disinhibiting effect is defined as how people say and do things in cyberspace that they would not ordinarily say and do in the face-to-face world. For further information, see; Suler, *The Online Disinhibition Effect*, 321–326.

[5] National Research Council, *Emerging Cognitive Neuroscience*, 27-28.

Threat Actors in Cyber Space

Every organization has a different threat perception consistent with their current position and capabilities. Each organization has different assets, threat levels and approaches. The design of these structures also differs between a private and a public organization, such as in the composition of cyber and physical elements in IT systems.

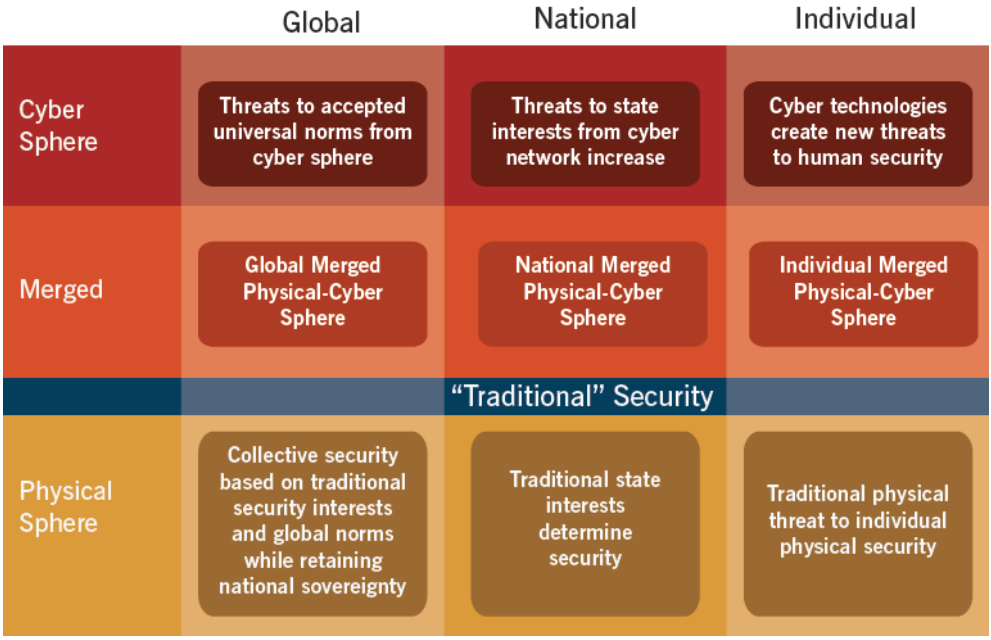


Figure 1: Threat Vectors[6]

While conducting this research, the main obstacle was to limit the good practices to all cyberspace. Disinformation campaigns and use of cyber space for terrorist purposes were out-with the scope of this research. Individual terrorist and groups use cyberspace for planning, training, recruitment, cooperation, financing and reconnaissance. In all these actions, cyberspace is used as a medium to facilitate their goals. However, in cyber space there are hardware, software and policies which regulate activities and functionalities. These infrastructures make services run for millions of people. Any service such as Twitter, Instagram or YouTube offers its programmed functionality for all users without knowing their intentions. As long as the messages of the users do not contradict the policies of the service provider, the platform will continue to serve to the user. The propaganda of individual terrorists and organizations is not the concern of this research. If terrorists decide to hack the platform or hack individuals in the same platform to have chances to distribute their message under other names or personas, then this would be in scope of this study.

[6] Fiddner, *Defining a Framework*, 12.

For example, on 23 April 2013, the Associated Press' Twitter account sent a message: "Two explosions in the White House and Barack Obama is injured." The message created a minor catastrophe in the stock markets[7] but it was later revealed that a group called the Syrian Electronic Army had captured the Twitter account of the Associated Press. The example demonstrates a case where Twitter should push the Associated Press to use two-level authentication and force its users to change their passwords periodically. Equally, Associated Press should be sensitive about phishing attempts to protect its reputation[8].

Capability Scale

Terrorists or terrorist groups could use cyberspace for three major different actions: enabling, disrupting and destructive acts. Basically, disruption and destruction attacks are those in which the perpetrators aim to halt the services or harm the target. In these types of attacks, terrorists target an asset in cyberspace to disrupt or destroy a service (or a computer-digital system) and the consequences of such an act would then appear in the kinetic world. In this research, however, we will concentrate on the types of attacks where terrorists target assets in cyberspace.

Enabling Acts

Terrorist groups use the online space for supporting publicity and propaganda efforts, recruitment, reconnaissance, clandestine communications between members, and disseminating their training manuals. These groups also utilize cyber-space as a training space for their followers. To prevent enabling acts requires different types of methodology and precautions, therefore these acts are kept out of this research.

Disruptive Acts

A second group of activities are those categorized as disruptive. Terrorist organizations may try to stop or interrupt IT services, disseminate malware, extract digital information, use denial of service attacks, or utilize phishing attacks. This group of attacks can also prepare the ground for destructive assaults. Recently there has been a remarkable increase in ransomware attacks, which could be categorized as a type of disruptive act. But the progress of ransomware can also quickly turn to a destructive act if the demands of the perpetrator are not met by the victims.

Destructive Acts

Destruction in cyberspace can also have consequences in the physical world. Destructive attacks harm IT infrastructure and stop the operation of the dependent services. High level attacks can target critical infrastructure facilities which could affect the daily life of people or services. Stuxnet (2010), Ukrainian Power Plant (2016), German Steel Mills (2014), New York Dam (2015), the Sadara Chemical Attack in Saudi Arabia (2017), the Bapco Attack in UAE (2020) and the Israel Water System Attack (2020) are major destructive attacks in cyberspace. There are also plenty of attacks where either the company tried to hide the event for reputational issues or the national government preferred to deny the incident.

7 Fisher, *Syrian hackers.*

8 Ingersol, *Inside the Clever Hack.*

In disruption and destruction acts, terrorists aim to intimidate or shock the audience by showing off their power and exposing the weakness of the alleged protectors of society. Any success would send a clear message to the public. Hardening the security of these services would increase the time or energy that the attacker has to spend on a particular attack. In most cases, the attackers prefer to find a less well hardened target to achieve their goal.

In risk management, the calculations for a particular system are built on two variables: threats and vulnerabilities. These two concepts are strongly associated in cyber security. Vulnerabilities and threats have different meanings from the perspective of defenders and attackers. Threats are quickly changing and levels alter from country to country. The asset (target) has no authority or control over threat levels. Since a cyber domain or system is made of several components, the owner of a facility could not have authority on threat levels. Therefore, harnessing threats is not the preferable method to follow for risk management. As clearly shown by Ucedavelez, "from an attacker's perspective, vulnerabilities are opportunities to attack an application to achieve specific goals such as stealing confidential information. A vulnerability such as weak encryption used to protect the data or weak authentication to access that data might facilitate a threat agent to access confidential data by brute forcing authentication and by performing an attack against the weak encryption used by the application[9]". From the defender's perspective, managing and reducing vulnerabilities is an efficient way for minimizing risks. Vulnerability is a common term used to define the security exposures in a network, operating system or other software or application software component in the system, as is human error (intentionally or accidently) within the organization.

Any vulnerability can potentially compromise the system or network if exploited. In this research, as a part of defining good practices in the defense against terrorism, we will focus solely on the vulnerabilities of computer systems. Computer systems in the cyber domain have various components such as hardware, software, data and a connection layer (fiber optics, land lines, etc.). There are major commonalities among computer systems but each computer system has certain differences. In computer systems, there are two sides: one is the attack surface and, trust boundaries is the other. Each computer system has different 'front-ends' and displays which form the attack surfaces. The attacker starts its mission by accessing the most convenient end. A large attack surface would increase the possibilities for an attack. To minimize the attack surface is generally either difficult or unreasonable. The second category, trust boundaries, represents the inside of the system, which tries to define trusted zones within an infrastructure. Trust boundaries are the critical spaces for a defender to reinforce and extend, and also the zone which would assist in threat modeling. In the conventional approach, minimizing the attack surface as much as possible, and securing and extending trust boundaries as much as possible are the principal rules. However, experience in the cyber security field demonstrates that the human element is also critical and they too have to be checked periodically to maintain security.

Protection and maintenance of cyber security for running systems will also reduce the effects of possible terrorist attacks. In cyber security literature, there are several methodologies for securing computer systems. In addition to differences in computer system structures, compiling good practices for securing the cyber domain is a very challenging task due to

[9] Ucedavelez and Morana, *Risk Centric Threat Modelling,* 635.

dynamic nature of the threat landscape. Even though the vendors are showing the utmost care in protecting their products, there is always a possibility of the presence of zero-day exploits, bugs and backdoors. In addition to these problems, human capital, those who are using these Information and Communication Technology (ICT) based systems, are also significant components in the system's security. Humans form the weakest link of in cyber security. All security measures have to be compatible with the rules of human-machinery interaction but most of the designs are not giving the required attention to the issue. For example, the computer access systems working with human interfaces have to be protected with an access policy. In most cases, in order to secure the systems, the length of password has to be long to prolong the duration required to achieve a successful brute force attack. However, the limitations of the human cognitive system and the 'business mindset' of efficiency often prevents the use of long and meaningless passwords.

Cyber Security Maturity Model

A changing threat landscape, different computer system structures and human inadequacies or malign intentions could be secured against terrorist attacks via adopting a macro cyber security approach. In the cyber security literature, there are several cyber security maturity models[10] being implemented across different sectors. In essence, a maturity model is an organized way to convey a path of experience, wisdom, perfection attributes, indicators or acculturation in a particular sector. The cyber security maturity model typically exemplifies good practices and may incorporate standards or other codes of practice of the discipline[11]. The cyber security maturity models also help to build a cyber security culture which would shape and focus the behaviors and codes of conduct of the human capital as well.

The major advantage of cyber security maturity models is in understanding security as a process which has to be repeated and renewed. In response to rapidly developing threats and vulnerabilities, the security of the computer systems is mostly comprehended by business owners as a task that has to be checked in to-do lists. However, ICT systems are similar to living organisms, which need continuous care and maintenance in accordance with daily dynamics. Any changes in the organizational structure or design of the systems has to be handled with the utmost oversight and restructured to meet the introduction of new system settings. These ICT mechanisms also have specific working conditions and durations which require a tailor-made change management strategy. The cyber security maturity models attempt to build a hierarchy and a documented process which aims to minimize vulnerabilities and build a proactive stance against any attacks, sabotage or accidents. In this paper, the cyber security maturity model is made up of ten domains: Risk management and Resilience planning; Asset, Change and Configuration Management; Identity and Access Management; Threat and Vulnerability Management; Situational Awareness; Information Sharing and Communications; Event and Incident Response; Continuity of Operations; Supply Chain and External Dependencies Management; Workforce Management; and Cyber Security Program Management.

[10] For a comparison of cyber security maturity models, see Rea-Guaman *et.al. Comparative Study,,* 100-113.

[11] Office of Cybersecurity, Energy, Security, and Emergency Response, *Cybersecurity Capability Maturity Model (C2M2) Program.*

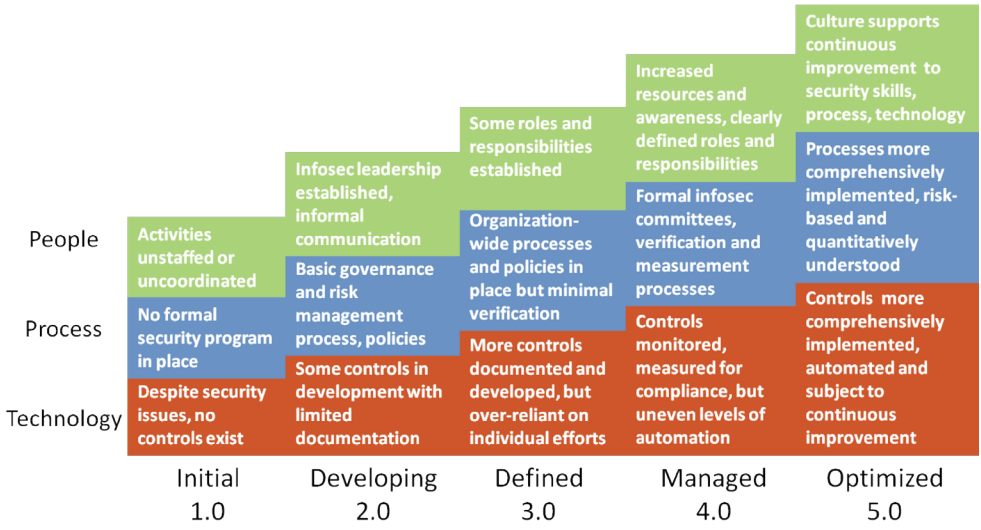


Figure 2: Another example of a maturity model[12]

Risk Management and Resilience Planning

The first step is to design the risk management systems and a resilience plan. The risk management domain aims to build up, operate and maintain a cyber security risk management program for your enterprise. This program will identify, analyze and mitigate the cyber security risks up to your requirements. It will also identify and understand risks for interconnected infrastructures and stakeholders. In recent years, the cyber security sector has reached a consensus that, given enough time and resources, every security technology is breakable; therefore, from the very first day the responsibility of the institution is to learn to build a resilient ICT technology. After all disruptions, either human made or natural hazard, all systems should be capable of maintaining their functionality and services. This should be the ultimate goal of all ICT systems from a defensive approach.

Leadership has a particular role in risk management. The leader defines the scope and prioritizes the functionality of the organization. In practice, the C-level hierarchy is responsible for the risk management of the organization. Generally the Chief Risk Officer (CRO) or Chief Security Officer (CSO) are responsible for operational risk management which in principle guarantees the functionality of the organization in case of or after a disaster or an attack. To achieve this role, the CRO and CSO has to follow a framework:

1-Prioritize and define the scope

The organization management has to define major functionalities and services of the organization which have to continue to be facilitated as much as possible. The C-Level have to make strategic decisions regarding the scope of the business.

[12] For further details, see Security Architect Partners, *How to Assess Security Maturity*.

2-Orient

The organization has to identify major threats (potential dangers) and vulnerabilities of the prioritized functionalities and services. This step requires comprehensive planning and strategic decisions to agree on "balanced security[13]".

3-Create a current profile

The organization has to take a snapshot of the current cyber security setting. An honest analysis of the setting will provide several indicators for the decision-makers about where to start.

4-Conduct a risk assessment

The organization has to make a risk assessment which will assist them in building a risk matrix. E.g., Failure Modes and Effects Analysis (FMEA) is one of the commonly used methodology in several industries[14]. Most sophisticated systems use information security management system (ISMS) which also includes a risk based approach in its design. It is also critical to underline that some of organizations have a strong belief in the risk matrix. However, major threats in the cyber security domain are non-linear risks, and indeed it is hard to measure them from a probability perspective. These matrices present quick solutions which relieve the responsible decision makers.

5-Create a target profile

Upon the assessment of your organizational risks, create a target cyber security level as an output. In this level, the costs and organizational energy requirements of the targeted level should be realistic and convenient to the strategy of the organization.

6-Determine, Analyze and Prioritize Gaps

To initiate the process, the organization should perform a gap analysis between the current and the desired status. The gap analysis would demonstrate major tasks and urgent requirements for the organization.

7-Implement Action Plan

Organizations should develop a timeline and a roadmap to fulfil the major tasks and requirements up to their level of urgency. In a functioning organization, the realization of these plans will always take more time than planned. In all these steps, there is a strong necessity to set milestones throughout the process to track improvement through assessments.

The final goal of Risk Assessment is reaching a certain level of resilience in the organization. The National Academies of Science (NAS) defined resilience as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events"[15] Thus, the organization would continue to function even in extreme times. (Figure 2)

---

[13] Harris and Maymi, *CISSP All-in-One,* 46.
[14] Asllani *et.al.*, *Strengthening information*.
[15] Kott and Linkov (eds.), *Cyber Resilience,* 3.

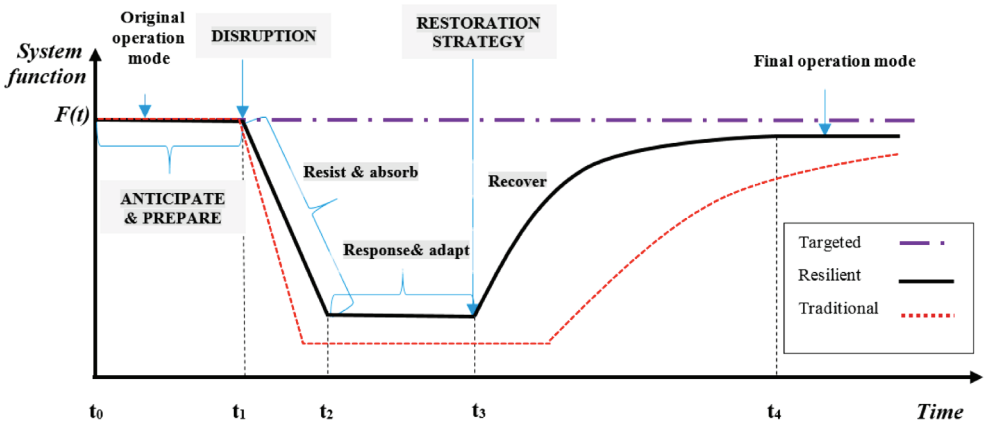


Figure 3: National Resilient Systems[16]

Asset, Change, and Configuration Management

The second domain is the identification of the relevant elements of asset and change management. In most institutions, the board, the CSO, the CRO or decision-makers have limited knowledge about their assets, something which could cripple their decision making process. Risk perception is one of the major factors in the protection of the institution. It also determines the budget allocation of the institution for security. The major goal of the asset, change, and configuration management is to manage the organization's IT and OT assets, including both hardware and software, relevant to the risk to critical infrastructures and organizational objectives. In some business oriented institutions, security is understood to be a one-time investment which would continue its functionality as long as it works. However, ICT systems are working in a complex environment which demands compatibility and high level association. To keep ICT systems up to date, a change management strategy is required which includes investment, management and implementation steps. Outdated technologies could create security problems as much as new technologies. There are reportedly nearly 1 million new malware threats released every day.[17] For example, if you are using Windows Server 2003, which reached the end of its support on July 2015, it means that you are at greater risk of cyberattacks and exploitation by third parties - or you are paying high prices to keep the server running[18].

The first step for securing the controls is to have vivid asset management. To sustain this goal automated asset management discovery tools have to be present in the organization. Regular and careful inspection will help the security management to prevent any unauthorized changes in the inventory. Another method to prevent unauthorized connection to the network is to activate Deploy Network Access Control (DNAC) with network level authentication via 802.1x.

[16] Bie *et.al. Battling the Extreme,* 1253–1266.
[17] Harrison and Pagliery, *Nearly 1 million.*
[18] Goldman, *Navy pays.*

Another major task for configuration management is patch management and security updates. Most unauthorized systems and applications typically use either the latest patches or security updates which were not installed in a timely manner. These systems are more vulnerable to exploitation.

A good example would be the JP Morgan Chase hack in 2014. As one of the largest banks in the US, this massive hack affected "the accounts of 76 million households and about seven million small businesses.[19]" The hackers acquired the list of bank's applications and programs on their computers. The attackers most probably cross checked all possible vulnerabilities of these programs and tested to find out an entry point into the bank's systems. Meanwhile, the bank's security team discovered the breach. But the hackers had already got the highest level of administrative privileges for the bank's several computer servers.

Identity and Access Management

The third step is identity and access management, which are critical for the physical and cyber security of institutions. As a follow up to Asset, Change, and Configuration Management, this step creates and manages identities, granting access to cyber or physical assets of the organization. To control access is a key point of interface between cyber security and HR departments. Several departments will be involved in this process within an organization. Most institutions will have a certain of degree trust in their workers. But the Fortinet report in 2019 demonstrates that there is a rising risk in all sectors from insider threats[20]. Inside the company is understood as in the limits of the trust boundary: thus, the focus on the staff is limited. It should be noted that not all cyber incidents occur as a result of malign intentions but sometimes a lack of expertise or basic training can cause accidents which cause unexpected results.

The cyber security management of organizations should centrally manage all accounts so as to have strong control on accounts. The relevant network and security devices should also use this centralized authentication system. Minimizing the number of privilege accounts will assist in the realization of security. These privileges should be regularly reviewed to prevent any possible problems and any account which cannot be associated with real person should be disabled. To tighten security, all accounts in the organization should have an expiration date which will help cyber security staff to manage privileges and the data hierarchy.

Another critical issue is weak passwords on employee or staff accounts in organizations. To reinforce the need for the staff to have strong passwords which contain capital letters, numbers and special characters is one of the methods applied in different sectors. Another preferred method of reinforcement is to force users to automatically re-login after a period of inactivity.

Due to practical usage and cognitive limitations, staff members often prefer to use simple passwords. The implementation of two-factor and/or two-channel authentication or hardware tokens and smart cards with certificates, one time passwords, or biometrics are other preferred methods by cyber security experts to reinforce access management security.

---

[19] Rushe, *JP Morgan Chase.*

[20] Fortinet, *Recognizing the Many Faces.*

Threat and Vulnerability Management

Fourth step is focused on threat and vulnerability management. This domain is one of the major components of the protection of the organization. The main goal is to establish and regulate plans, procedures and checklists and to implant the necessary technologies to detect, identify, analyze and manage cyber security threats and vulnerabilities compatible with the strategy of the organization. In this element, institutions have to decide about their level of protection. It is not feasible to establish a protection regime against all threats. Some threats are more urgent and more likely than others. Each organization has a different structure and range of software. Threat management requires several components: firewalls, anti-malware, anti-spam, IDS/IPS, content filtering, data leak prevention, VPN capabilities, as well as continuous monitoring and reporting. The observation and response to these threat layers is very problematic. One of the simplest solutions is unified threat management (UTM) appliance products which are developed to combine several functionalities in a sole network appliance. The UTM appliances are mostly designed from a point of view of holistic security management. But exclusive capacity UTM appliances quickly turn to a disadvantage if the hackers have compromised the control. It would require a risk-based approach to deploy another protection level to prevent this scenario.

To understand the possible risks in different operating systems and digital components, organizations would use a risk (reporting) matrix (see Figure 1) to calculate possible threats and vulnerabilities for their structure. The visualization and probability calculation of the risks would help decision-makers make their judgement[21].

Figure 4: Risk Matrix[22]

IMPACT ⇨ LIKELIHOOD ⇩	Negligible	Minor	Moderate	Major	Catastrophic
Remote	Very Low Risk	Low Risk	Low Risk	High Risk	Very High Risk
Unlikely	Very Low Risk	Low Risk	Moderate Risk	High Risk	Very High Risk
Possible	Low Risk	Moderate Risk	Moderate Risk	High Risk	Very High Risk
Likely	Low Risk	Moderate Risk	High Risk	Very High Risk	Very High Risk
Certain	High Risk	High Risk	High Risk	Very High Risk	Very High Risk

[21] U.S. Department of Defense, *Risk, Issue and Opportunity Management Guide.*
[22] Bukowski, *Logistics decision-making*, 65-79.

Risk reduction begins with collecting and analyzing the vulnerability of the information in your organization, which would then clarify your threat actors and their intentions. There are studies in threat management that cluster possible threats. Major security problems in cyber security are grouped as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege[23]. There are also several methodologies, but MITRE ATT&CK gives us a detailed roadmap on how an attacker would proceed[24].

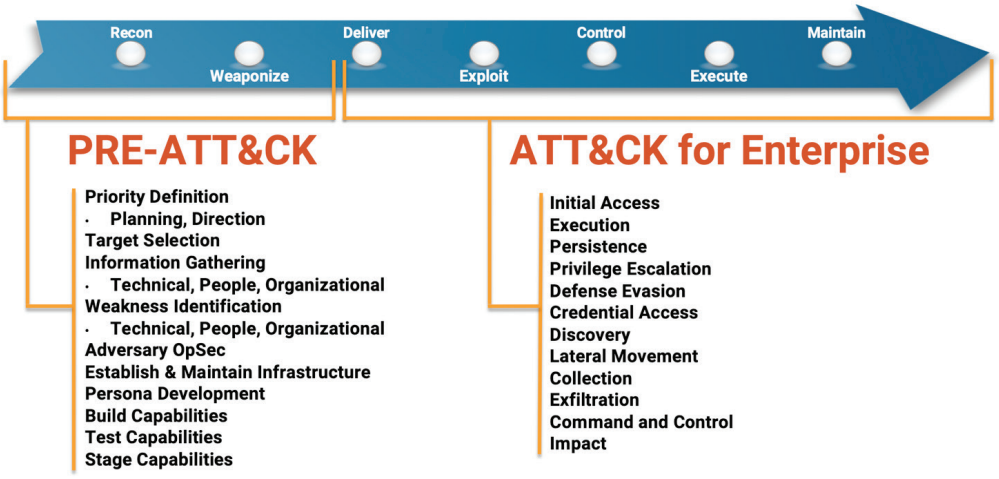


Figure 5: MITRE ATT&CK - Kill Chain[25]

Situational Awareness

The main goal of this domain is to establish technologies to collect, analyze and warn operators when to obtain status and summary information regarding the operational cyber security condition. The ultimate goal is to form a Common Operating Picture (COP) to be effective in decision making, staff actions, and appropriate mission execution in complex and dynamic environment of the organization's cyber security setting. Bennet defines situational awareness as "the knowledge of where you are, where other friendly elements are, and the status, state, and location of the enemy.[26]" He also categorized "the levels of situational awareness":

Level 1 situational awareness involves perceiving the critical factors in the environment.

Level 2 situational awareness is understanding what those factors mean, particularly when integrated together in relation to the decision maker's goals.

Level 3 situational awareness is the highest level, which is an understanding of what will happen with the system in the near future."[27]

---

23 Shostack, *Threat Modeling*.
24 Mitre Attack, *Enterprise Matrix*.
25 *Ibid.*
26 Bennett, *Understanding, Assessing,* 292.
27 *Ibid*.

In an organization, if COP suggests a need for heightened security, then visitors may be screened more carefully, the Helpdesk may conduct malware scans on misbehaving laptops, and human resources might send out reminders about phishing. Senior management reviews the COP and the cyber response teams should be prepared to take extraordinary action such as shutting down the website, if necessary. At the highest state of alert, they can change firewall rule sets to restrict nonessential protocols like video conferencing, delay all but emergency change requests, and put the cybersecurity incident response team on standby[28].

Information Sharing and Communications

The cyber hygiene of an organization is relevant within its ecosphere. Since the organization is working in an interconnected and complex environment, to warn the relevant parties and learn of recent security developments is critical for protection. To establish and maintain relationships with internal and external entities, and to collect and provide cybersecurity information would in most cases reduce risks and increase the operational resilience of the organization. Information sharing practices will help organizations to be informed about the rising risks and also to gain insights regarding their vulnerabilities. The information sharing practices also refine the communication skills of the involved parties which might be relevant in the case of an emergency. To decide what to share and how to share would also reinforce organizational communication skills and expedite the decision-making process.

There are several pieces of research on information sharing for mitigating attacks. Microsoft's research presents eight recommendations for information sharing:

1. Develop a strategy for information sharing and collaboration.

An information sharing strategy can help organizations: identify priorities, establish shared values, and plan to build effective information sharing processes.

2. Design with privacy protections in mind.

Information sharing efforts must respect privacy, and should be designed with the aim of protecting this to the highest degree.

3. Establish a meaningful governance process.

A meaningful governance process should include appropriate management of the data shared, from its creation and release to its use and destruction.

4. Focus sharing on actionable threat, vulnerability, and mitigation information.

Sharing actionable information empowers organizations to improve their defense of networks and mitigate threats.

5. Build interpersonal relationships.

Building trust between information sharing participants, along with trust in the program itself, is critical. The more that information sharing participants act in good faith, the more likely other participants are to share information on threats and vulnerabilities.

[28] Office of Cybersecurity, Energy, Security, and Emergency Response, *Cybersecurity Capability*, 30.

6. Require mandatory information sharing only in limited circumstances.

In some instances, such as in the case of national security and public safety, there may be a need for mandatory incident reporting.

7. Make full use of information shared, by conducting analyses on long-term trends.

The analyses of trends gleaned from shared information can help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and helping them defend against or prevent future threats.

8. Encourage the sharing of good practices.

The exchange of good practices with peer organizations can allow organizations to play a proactive role, by engaging with each other as well as external organizations[29].

Event and Incident Response, Continuity of Operations

This domain is highly interconnected with situational awareness. The monitoring capacities of the organization would continuously observe operations when they detected an escalation in any level of operations, and they will define a suspicious incident and quickly react to support the security of the organization. This domain has five major steps to follow:

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events and Declare Incidents
3. Respond to Incidents and Escalated Cybersecurity Events
4. Plan for Continuity
5. Management Activities

In some OT environments, responding requires specification on a certain environment (e.g., SCADA[30]) in which case, the organization has the responsibility to find ways to build up required training and to cultivate the necessary levels of experience among its staff.

Supply Chain and External Dependencies Management

Today, the cyber security element of an organization is highly connected with other organizations' particular functions and IT environments. This interdependence among infrastructures, operating partners, suppliers, service providers, and customers is also increasing. Supply chain cyber security experts discuss extensively how to mitigate and manage the third party risks. The organization should identify these third-party risks and form a management plan for this domain as well. When we realize that cyber security devices and other IT/OT hardware are mostly obtained by third-parties, we understand the criticality of the management of supply chain and external dependencies.

---

29 Goodwin and Nicholas, *A Framework for Cybersecurity*.

30 SCADA stands for Supervisory control and data acquisition which formed by software and hardware components. SCADA mainly use for control industrial processes, monitor real-time data, directly interact with sensors, valves, pumps, etc.

Workforce Management

In the cyber security chain, the most significant issue is workforce management. The maturity of the cyber security program in an organization is only possible through the construction of a robust security culture. This domain aims to ensure the ongoing suitability and competence of personnel in all departments, so that they have the required level of awareness and the proper training to sustain security. Organizations might have high reliance on technology, but the staff is critical when it comes to utilizing cyber security equipment. High levels of expertise and training in staff would harden the protection level and also expand trust boundaries.

Cybersecurity Program Management (CPM)

Action in all domains is necessary to establish the cyber security maturity model, but a cyber security program and its implementation is as crucial as all the other steps. The CPM decides on the appropriate policies and focuses on the execution of these policies, including strategic planning. As C2M2 manual clearly notes, "a cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or the function"[31]. The higher management of the organization has to be involved in the formation of the CPM process (see Figure 6) and the policies have to be in line with the management policy. In case of a change in the high-level management, the new management personnel should revise the organization's CPM strategy to the most recent management approach. A sophisticated CPM should be regularly updated in terms of its outlook on people and policy risks, as well as operational and technological risks. The management should also focus on the introduction of these updates to the workforce and the integration of them into its security culture. On the other hand, the CPM should be consistent within the framework of state-level regulations and approaches.

The CMP cycle demonstrates that management should be vigilant in following the cycle to mature its strategy and its cyber security outlook.

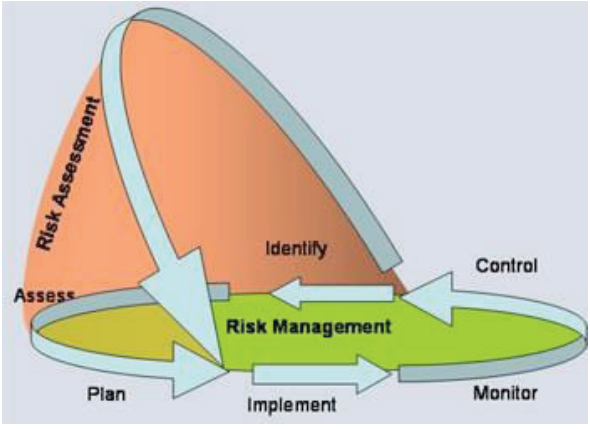


Figure 6: CPM cycle[32]

[31] Office of Cybersecurity, Energy, Security, and Emergency Response, *Cybersecurity Capability,* 46.
[32] ENISA, *Risk Management*.

Conclusion

To conclude, this research intends to elaborate upon the cyber security maturity domains which will strengthen a computer system's infrastructure against any terrorist attack. The implementation and constant improvement of the cyber security maturity model will reinforce the security of the organization. In the ICT sector, the maturation of security should be understood as one of the most effective practices in countering terrorism in cyberspace. The repetition of good practices and necessary adjustments to the nature of your organization is the key for success. The ultimate achievement is to transform these steps of cyber security maturity into a security culture which is unique to your organization. To list these domains is easier than to exercise them. The execution of such a project requires the total involvement of all parties and partners in the organization to achieve this goal. All of the domains for cyber security maturity model interact with each other. A strict implementation of these strategies would also minimize the possibilities for the use of cyber space for terrorist purposes. Any gap within a domain or disconnection amongst them will harm the overall process. Cyber security is not a solely information security question but a multidimensional issue, involving the interaction of multiple actors, policies, laws and regulations. It is a shared responsibility and it builds trust in an organization, in a corporation or in a public entity. Functionality is sustained by security and through trust between all the relevant participants. The management of the process also demands a remarkable amount of energy and attention from the executive level. The laboriousness and seeming passive stance of defense can deplete motivation and excitement across all levels of cyber security officials. But the C-Level management has to give special attention to security management with a particular focus on human psychology to meet this challenge. But the hardest task is to transform all these security steps into a robust and vivid security culture within the organization. Otherwise, the ICT infrastructure will be an easy target for terrorists.

Bibliography

Anderson, Ross, (2008), *Security Engineering: A Guide to Building Dependable Distributed Systems*, (Indiana: Wiley)

Asllani, Arben, Lari, Alireza, and Lari, Nasim, (2018), "Strengthening information technology security through the failure modes and effects analysis approach", *International Journal of Quality Innovation*, Vol. 4, No. 5, https://jqualityinnovation.springeropen.com/articles/10.1186/s40887-018-0025-1. (Accessed 15 December 2020)

Bennett, Brian T., (2007), *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, (Indiana: Wiley).

Bie, Zhaohong, Lin, Yanling, Li, Gengfeng, and Li, Furong, "Battling the Extreme: A Study on the Power System Resilience", *Proceedings of the IEEE*, Vol. 105, No.7, 2017, pp. 1253–1266.

Bukowski, Lech, (2019), "Logistics decision-making based on the maturity assessment of imperfect knowledge", *Engineering Management in Production and Services*, Vol. 11, No. 4, pp. 65-79.

Cavelty, Myriam Dunn, (2013), "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse", *International Studies Review*, Vol. 15, No. 1, pp. 105-122.

Choucri, Nazli, (2012), "Emerging Trends in Cyberspace: "Dimensions & Dilemmas", in Phil Williams and Dighton Fiddner (eds.), *Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*, (United States Army War College Press).

European Union Agency for Cybersecurity (ENISA),"Risk Management & Information Security Management Systems", https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms. (Accessed 15 December 2020)

Fiddner, Dighton, (2015), "Defining a Framework for Decision-Making in Cyber Space", *IBM Center The Business for Government*, http://www.businessofgovernment.org/sites/default/files/Defining%20a%20Framework%20for%20Decision%20Making%20in%20Cyberspace.pdf. (Accessed 15 December 2020)

Fisher, Max, (2013), "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?" *Washington Post*, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/. (Accessed 15 December 2020)

Fortinet, "Recognizing the Many Faces of Insider Threats", 2019, https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-recognizing-the-many-faces-of-innsider-threats.pdf. (Accessed 15 December 2020)

Goldman, David, "Navy pays Microsoft $9 million a year for Windows XP", CNN Business, 26 June 2015, https://money.cnn.com/2015/06/26/technology/microsoft-windows-xp-navy-contract/. (Accessed 15 December 2020)

Goodwin, Christin, and Nicholas, J. Paul, (2015), "A Framework for Cybersecurity Information Sharing and Risk Reduction", *Microsoft*, https://www.microsoft.com/en-us/download/confirmation.aspx?id=45516. (Accessed 15 December 2020)

Harris, Shon, and Maymi, Fernando, (2019), *CISSP All-in-One Exam Guide,* Eighth Edition, (New York: McGraw-Hill Education).

Harrison, Virginia, and Pagliery, Jose, (2015), "Nearly 1 million new malware threats released every day", CNN, 14 April 2015, https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html. (Accessed 15 December 2020)

Ingersol, Geoffrey, (2013), "Inside the Clever Hack That Fooled The AP And Caused The DOW To Drop 150 Points", *Business Insider*, https://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-the-ap-and-caused-the-dow-to-drop-150-points-2013-11. (Accessed 15 December 2020)

Kott, Alexander, and Linkov, Igor (eds.), (2019), *Cyber Resilience of Systems and Networks*, (Springer), E-Book.

Mitre Attack, "Enterprise Matrix", https://attack.mitre.org/matrices/enterprise/. (Accessed on 15 December 2020)

National Research Council, (2008), *Emerging Cognitive Neuroscience and Related Technologies*, (Washington, DC: The National Academies Press)

Office of Cybersecurity, Energy, Security, and Emergency Response, "Cybersecurity Capability Maturity Model (C2M2) Program", https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0. (Accessed 15 December 2020)

Rea-Guaman, Angel Marcelo, San Feliu, Tomás, Calvo-Manzano, Jose, A. and Sanchez-Garcia, Isaac Daniel, (2017), "Comparative Study of Cybersecurity Capability Maturity Models", Conference Paper presented at Software Process Improvement and Capability Determination, pp. 100-113.

Rushe, Dominic, (2014), "JP Morgan Chase reveals massive data breach affecting 76m households",

The Guardian, 03 October, 2014, https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach. (Accessed 15 December 2020)

Security Architect Partners, (2020), "How to Assess Security Maturity and Make Improvements", 16 February 2020, https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/. (Accessed 15 December 2020)

Shostack, Adam, (2014), *Threat Modeling: Designing for Security*, (Indiana: Wiley)

Suler, John, (2004), "The Online Disinhibition Effect", *CyberPsychology & Behavior*, Vol. 7, No. 3, pp. 321–326.

U.S. Department of Defense, (2017), "Risk, Issue and Opportunity Management Guide for Defense Acquisition Programs", Office of the Deputy Assistant Secretary of Defense for Systems Engineering, http://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf. (Accessed 15 December 2020)

Ucedavelez, Tony and Morana, Marco, (2005), *Risk Centric Threat Modelling: Process for Attack Simulation and Threat Analysis*, (Indiana: Wiley).

CHAPTER V

BEST PRACTICES FOR STRENGTHENING THE PROTECTION OF NATO AND PARTNER NATION CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS: *IT IS ALL ABOUT THE "HOW"*

Ronald Bearse

"Critical infrastructure protection needs to be understood as not only deploying a tougher exoskeleton, but also developing organizational antibodies of reliability that enable society and its constituent parts to be more resilient and robust in the face of new, dynamic, and uncertain threats"[1]

Introduction

The pace with which modern economies have become intrinsically interconnected over the course of the last 20 years, particularly in the information and communications sectors, has exposed our societies to a set of unprecedented threats and vulnerabilities. Many of these come from terrorist groups that seek to destabilize communities and create widespread panic by interfering in those very systems, assets, and processes which our societies depend on for their survival. These assets and processes are often referred to as "critical infrastructure".[2]

Critical infrastructure represents a vast, global sector. It is therefore not possible to always ensure its full protection and in all places. Unfortunately, it is likely that some terrorist attacks against critical infrastructure will succeed. A useful component of a comprehensive strategy to protect critical infrastructure is the capacity to minimize the impact of terrorist attacks through adaptation - impact reduction, responses to emergencies, and recovery. The physical protection of the target also involves reduction of the impact if the attack takes place.

The last 20 years has also seen an increase in the number of terrorist attacks, necessitating the development of more efficient global security policies. One of the most important elements of this enhanced security is the protection of critical infrastructure. However, despite the efforts of national security entities in the national and international context, terrorist attacks will never be completely preventable, so the "protection" of critical infrastructure is evolving to encompass the concepts of "security and resilience" to ensure specified levels of operational performance pre-, trans- and post-attack.

1 Auerswald et. al., *The Challenge of Protecting.*
2 United Nations, *The Protection of Critical Infrastructure*, 14.

The next few paragraphs briefly cover the NATO definition of critical infrastructure, the increasing risks to critical infrastructure, the evolution of critical infrastructure protection and identify the major stakeholders involved in this vital component of national and economic security. Following these brief topics, the remainder of this chapter: (1) defines the nexus that exists between the critical infrastructure security and resilience and counterterrorism communities; (2) defines good practices for fostering the communication, cooperation, collaboration, coordination and concentration ("the how") required to effectively perform critical infrastructure security and resilience work streams; and (3) provides recommendations for strengthening NATO's capability and capacity to assist Alliance members and partner nations in applying good practices and valuable and costly lessons learned in developing and implementing critical infrastructure security and resilience policies.

NATO Definition of Critical Infrastructure

Even though each nation determines that which constitutes its critical infrastructure, many nations have identified a common understanding.

For example, the European Commission defines critical infrastructure as physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.[3]

Europe's critical infrastructures are highly connected and highly interdependent. Corporate consolidation, industry rationalization, efficient business practices such as just-in-time manufacturing and population concentration in urban areas have all contributed to this situation. Europe's critical infrastructures have become more dependent on common information technologies, including the internet and space-based radio navigation and communication. Problems can cascade through these interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services. Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction.[4]

NATO defines critical infrastructure (CI) as "those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government."[5]

Infrastructure deemed critical can vary according to a nation's needs, resources, and development level. Examples of CI defined in many nations all over the world include the

[3] European Commission, *Critical Infrastructure*.
[4] Eur-Lex, *Critical Infrastructure Protection*.
[5] Jahier, *Critical Infrastructure*.

systems, assets, facilities, and networks found in important industry sectors such as energy, transportation, water, communications, information technology, food and agriculture, and emergency services, and banking and finance, to name but a few.

CI is diverse and complex and includes distributed networks, varied organizational structures and operating models (including multi-national ownership), interdependent functions and systems in both physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations.[6]

Risks to Critical Infrastructure are increasing

Terrorists and terrorist organizations have increasingly shown interest in attacking critical infrastructure and recent attacks have exposed the intrinsic vulnerabilities of several critical infrastructures in a variety of sectors, such as energy, transportation, water and communications.[7] Recent attacks on transportation systems, repeated acts of sabotage against dams, oil pipelines, bridges, etc., by Al-Qaida and ISIL indicate the continued interest of terrorist groups in disrupting critical infrastructure.[8]

From an operating perspective, CI is increasingly interdependent and vulnerable due to the nature of its physical environment, functionality, supply chain, and cyber interconnections. Moreover, since many such facilities and networks operate across borders, any terrorist attack against them could certainly have regional and global implications.

Any number of factors can cause disruptions: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightning strikes, etc.) or physical destruction due to intentional human actions (theft, arson, terrorist attack, etc.). Of particular concern is the fact that the growing complexity and interconnectedness of CI means that a disruption in one may lead to disruptions in others.[9]

For example, energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors, and, in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication). A terrorist attacks against one of these sectors can impact another sector.[10]

Similarly, a terrorist attack on a rail or aviation hub can rapidly mushroom into a damaging stoppage of essential human and commerce links. Add to this the fact that trains often carry substantial amounts of hazardous materials, sometimes in remarkably proximity to large concentrations of people and industry, and transportation networks are a prime axis of vulnerability, requiring constant attention and resources. Maritime hubs present no less of a threat. Every shipping container is a potential guided missile and should be treated

6 Domestic Preparedness, *Critical Infrastructure.*
7 United Nations, *The Protection of Critical Infrastructure*, 22.
8 Ibid.
9 Ibid.
10 Cyber Security & Infrastructure Agency (CISA), *A Guide to Critical Infrastructure*.

as such. A remote-controlled detonation of a container loaded with radiological waste products, such as those produced by every large-scale hospital around the world, can spread enough contamination and fear to freeze a huge seaport for months if not years, exacting an incalculable economic and psychological impact.[11]

There are several other colliding factors which have increased the risks to CI.[12] , including:

- The diminishing governmental control due to liberalization and privatization of infrastructures.
- The increased use of information and telecommunication technologies (ICT) to support, monitor, and control CI functionalities.
- The demands of the population that services can and shall be available 24/7.
- Urbanization which stresses the utilization of old infrastructures to their limits.
- The increasing interwovenness, (supply) chaining and dependencies of infrastructural services.
- Adversaries of the society who increasingly understand that a successful attack may create havoc.
- Many nations increasingly depend on CI partially or completely located outside their jurisdiction and over which they have little or no control.[13]

When looking at the totality of the factors which have increased the risks to CI, it should be no surprise that all CI cannot be "protected" from all "hazards" (be they terrorist attacks or other disruptive/destructive natural and man-made events) at all times. Therefore, the concept of critical infrastructure protection (CIP) has been superseded by the concept of critical infrastructure security and resilience (CISR) which involves a wide range of stakeholders.

From CIP to CISR and Key Stakeholders

Over the course of the last decade, many nations have evolved their CI policies and strategies to focus more on security and resilience than protection.

Security may be defined as reducing the risk to critical infrastructure from intrusions, terrorist attacks or the effects of natural or man-made disasters, through the application of physical means or defensive cyber measures. Organizations implement security in diverse ways, including both physical and cybersecurity measures. Examples of which include:

- Installing identification badge verification at doorways
- Using security fencing around buildings
- Deploying network monitoring tools
- Locking devices (such as laptops and cell phones) when not in use

[11] Tal, *America's Critical Infrastructure*.
[12] Setola et. al., *Critical Infrastructures*.
[13] Clemente, *Cyber Security*.

Resilience may be defined as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. The effectiveness of resilient critical infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event, including a terrorist attack. As with security, there are both physical- and cyber-resilience strategies organizations can undertake, such as:

- Having a backup power generator
- Developing a business continuity plan
- Building with materials appropriate to the area's natural risks
- Implementing annual cybersecurity training for employees

CISR is a shared responsibility between many stakeholders — from the private sector owners and operators of critical infrastructure and various national, regional and local government and non-government entities' (including industry associations, higher education and research and development organizations). Roles and responsibilities for maintaining or improving the security and resilience of critical infrastructure vary widely and are affected by many factors such as: public versus private ownership; regulations within a sector; anticipated threats and hazards to a specific sector; and decisions on whether the sector or region chooses to focus on taking actions to protect infrastructure, reduce consequences, or rapidly respond to and recover from adverse events.[14]

The CISR and Counterterrorism (CT) Community Nexus

The transnational nature of terrorism requires a coordinated response of all states and actors of the international community. For many years, international counterterrorism cooperation was limited in the area of CIP/CISR. However, in recent years, there have been several international programs/initiatives developed by the organizations/nations to support the protection of CI against terrorist attacks and other hazards, including those listed below:

- The European Union's "European Program for Critical Infrastructure Protection" [15]
- The Organization of American States "Protection of Critical Infrastructure against Emerging Threats" and "Tourism Security Program"[16]
- NATO's "Energy Security" and "Civil Emergency Planning" efforts"[17]
- INTERPOL's Major Event Support Teams (IMEST)[18]
- INTERPOL's Incident Response Teams (IRT)[19]
- OSCE's "Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks" and Regional Cooperation Council "Integrated Infrastructure Planning"[20]

---

14 CISA, *A Guide to Critical Infrastructure.*
15 European Commission, *Protection*.
16 Organization of American States (OAS), *Tourism Security Program*.
17 Rühle, *NATO and Energy Security*.
18 INTERPOL, *Focus: Interpol Major Events*.
19 Ibid.
20 OSCE, *Good Practices*.

- The United Nations' Counterterrorism Implementation Task Force (CTITF) Working Group on Protection of CI[21]
- The Council of Europe's Budapest Convention and Related Standards[22]
- The UN's Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[23]
- Information Sharing and Analysis Centers (ISAC)[24]

These programs and initiatives are important to reference because, either singly or collectively, they have helped:

- Raise awareness of the threats to CI
- Facilitate technical assistance in many CISR areas
- Support the analysis and assessment of counterterrorism trends
- Address the prevention, preparedness, mitigation, investigation, response, recovery and other relevant aspects of CIP/CISR
- Reflect renewed willingness on the part of the international community to elaborate upon and upgrade mechanisms needed to minimize the risks to CI caused by terrorist attacks and adequately respond to, and recover from, such attacks
- Spotlight the fact that several nations have chosen to adopt broad and integrated strategies which take into consideration the need to enhance CI resilience against all hazards

Cooperation between the CISR and CT Communities is increasing

At the 2016 Summit in Warsaw, Allied leaders committed to continue enhancing national resilience to further develop their individual and NATO's collective capacity to resist any form of armed attack. The Alliance committed to continue to enhance its resilience against the full spectrum of threats, including hybrid threats, from any direction. It agreed to strive to achieve the agreed requirements for national resilience by protect their populations and territory by strengthening continuity of government, continuity of essential services and security.[25]

In May of 2016, NATO conducted an Advanced Research Workshop, "Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges", held in Stockholm, Sweden. The main objective of the workshop was to help and support NATO in the field of hybrid conflicts by developing a set of tools to deter and defend against adversaries mounting a hybrid offensive. Addressing the current state of CIP and the challenges evolving in the region due to non-traditional threats which often transcend national borders – such as terrorist attacks on energy supply – a wide range of international experts provided solutions from several perspectives to counter the new and emerging challenges affecting the security of modern infrastructure.[26]

---

[21] https://www.un.org/counterterrorism/ctitf/en/protection-critical-infrastructure-including-vulnerable-targets-internet-and-tourism-security

[22] Council of Europe, *Budapest Convention*.

[23] United Nations General Assembly, *Developments in the Field*.

[24] National Council on Information Sharing and Analysis Centers (ISACs), *ISACs*.

[25] NATO HQ, *Commitment to Enhance Resilience*.

[26] Niglia (ed.), *Critical Infrastructure Protection*.

In 2017, UN Security Council Resolution 2341 was adopted as the first ever global instrument entirely devoted to the protection of critical infrastructure against terrorist attacks. Its provisions reflected renewed willingness on the part of the international community to elaborate and upgrade mechanisms needed to minimize risks to critical infrastructure caused by terrorist attacks and to respond to and recover from such attacks. The resolution also invites Member States to consider possible preventive measures in developing national strategies and policies. This Resolution, the UN Global Counter-Terrorism Strategy, and other international conventions and protocols against terrorism provide the framework for NATO's efforts to combat terrorism.[27]

The Warsaw Summit laid the groundwork for the Alliance to bolster resilience, with the development of evaluation criteria in 2017 to support nations in conducting national resilience self-assessments, followed by a NATO assessment of the overall state of the Alliance's civil preparedness in 2018. This identified areas for further work and NATO is supporting Allies by providing guidelines on how to increase the level of preparedness across the seven baseline requirements.

NATO Civil Emergency Planning, Centers of Excellence, and Counterterrorism Efforts Focused on CIP/CISP

NATO Civil Emergency Planning is a national responsibility within NATO so there is no centralized planning. The aim is to create a framework for nations to ensure compatibility and effectiveness of national arrangements, enable them to assist each other when needed, and ensure civil support to NATO objectives.[28] In support of the maintenance of a collective defense capability, NATO Civil Emergency Planning:

- Provides advice to the Alliance on all matters related to civil preparedness.
- Supports NATO's overall crisis prevention and management arrangements.
- Cooperates with and supports the military in peace, crisis, and war.
- Ensures the functioning of government in crisis and war.
- Ensures an acceptable level of social and economic life in crisis and war; and
- Supports and protects the population in crisis and war.[29]

NATO Civil Emergency Planning is part of the Operations Division under the International Staff at NATO Headquarters, coordinates efforts with Allies and partner nations include dealing with "left of bang" requirements (such building situational awareness and readiness prior to potential incidents or attacks), as well as "right of bang" requirements (such as managing the consequences of incidents and attacks).

NATO Civil Emergency Planning is primarily concerned with aspects of national planning that affect the ability to contribute to Allied efforts in continuity of government, continuity of essential services to the population, and civil support to military operations. These three critical civilian functions have been translated into the following seven baseline "resilience-building" requirements:

---

[27] NATO HQ, *Relations with the United Nations*.
[28] Fausboll, *NATO Civil Emergency Planning (CEP)*, 10.
[29] NATO HQ, *Civil Emergency Planning*.

- Assured continuity of government and critical government services
- Resilient energy supplies
- Ability to deal effectively with uncontrolled movement of people
- Resilient food and water resources
- Ability to deal with mass casualties
- Resilient civil communications systems
- Resilient transportation systems

Together with a package of protection guidelines, assessments and a tailored toolbox, Civil Emergency Planning's objective is to support Alliance nations in building greater resilience and providing benchmarks against which to assess these seven states of civil preparedness to strengthen CISR in what are often referred to as the "life-line" CI sectors underlined above. This is vital work, since lifeline infrastructure sectors have a set of defining characteristics which separate them from other sectors and the services they provide. In general, there are four main factors that define lifelines:

- They provide necessary services and goods that support every home, business, and county agency.
- Lifelines deliver services that are commonplace in everyday life, but disruption of the service has the potential to develop life-threatening situations.
- They involve complex physical and electronic networks that are interconnected within and across multiple sectors.
- A disruption of one lifeline has the potential to effect or disrupt other lifelines in a cascading effect.[30]

In 2020, in the context of the COVID-19 pandemic, NATO took necessary measures to ensure that any movement of military assets did not unwittingly contribute to the spread of the virus. For this reason, NATO began monitoring the movement situation closely and worked with Allies and partners accordingly. In this respect, and in learning lessons from the COVID-19 pandemic and other challenges such as emerging and disruptive technologies and climate change, NATO is seeking to strengthen the resilience of Allied societies.[31]

To deter, counter or recover from threats or disruptions to the critical infrastructure, effective action requires clear plans and response measures, defined well ahead of time and exercised regularly.

In addition to the NATO Civil Emergency Planning activities briefly outlined above, a few NATO Centers of Excellence have also been supporting CISR efforts in Alliance and partner nations.

---

[30] National Association of Counties, *Protecting Critical Infrastructure*.
[31] NATO HQ, *Civil Preparedness*.

NATO Centers of Excellence Efforts

NATO accredited Centers of Excellence play a significant role in the domains of innovation, education and training, doctrine, and capability development, through experimentation and recommendations. They are also hubs, in their respective domains, for the enhancement of Allies and partners interoperability, where NATO Allied Command Transformation plays a key role, along with innovation, to ensure that we remain capable of operating together. NATO Centers of Excellence have also proven to be a very practical way to foster NATO and European Union cooperation. For example, the Joint Chemical, Biological, Radiological, and Nuclear Center of Excellence. [32]

NATO Centers of Excellence are not part of the NATO Command Structure but form part of the wider framework supporting NATO Command Arrangements. Centers of Excellence are nationally or multi-nationally sponsored entities, which offer recognized expertise and experience to the benefit of the Alliance, especially in support of transformation, which gives them great flexibility in the relationships they have with other international and civilian entities.[33]

The Energy Security Center of Excellence has developed a "Critical Energy Infrastructure Protection" course to support national authorities in protecting critical energy infrastructure, as well as enhancing their resilience against energy supply distributions that could affect national and collective defense, including hybrid and cyber threats.

The NATO Cooperative Cyber Defense Center of Excellence supports NATO with unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy, and law.

The NATO Crisis Management and Disaster Response Center of Excellence offers a "Crisis Management and Disaster Response" course which covers, among other topics, NATO CEP and Crisis Response Planning; resilience and civil preparedness against current and future threats to security; and outlines the NATO resilience baseline requirements identified above and the criteria for evaluating them.

The NATO Center of Excellence Defense Against Terrorism is an internationally recognized and respected resource for terrorism expertise. It serves as the hub of a wide network of international military, government, non-government, industry, and academic communities of interest.

Since 2013, 500 students have attended the Critical Infrastructure Protection Against Terrorist Attacks course. This course was designed to raise awareness of the growing threat to critical infrastructure, share valuable lessons learned, present case studies and practical tools, and discuss major trends, issues, concerns impacting the development of critical infrastructure protection policies, plans and procedures.

---

[32] Ibid.

[33] NATO HQ, *COE Catalogue*.

The Critical Infrastructure Protection Against Terrorist Attacks course is being modified to deliver better content in the form of case studies and practical tools to better serve NATO's long-term interests in this area. Taught by a wide selection of top-notch public and private sector practitioners from around the world, this course provides a unique educational platform for:

- Exposing students to the essential elements of modern national CIP/CISR policy and planning
- Discussing how CIP/CISR supports national and economic security, as well as economic prosperity
- Focusing on all critical infrastructure sectors, particularly energy and transportation
- Increasing student knowledge and understanding of current and emerging issues, concerns and challenges in developing and implementing national CIP/CISR policy and plans
- Identifying the roles and responsibilities of government, the private sector, non-government organizations, international organizations, and others in protecting critical infrastructure
- Emphasizing the need for clear and unambiguous methods for defining risk terms and risk methodologies for use in protecting critical infrastructure against terrorist attack
- Providing students with concepts, methods and tools which can be used to improve the protection of critical infrastructures in their countries
- Explaining the essential need for public-private partnerships and information sharing mechanisms for protecting critical infrastructure; and for
- Providing an immersive practicum that enables students to apply what they learned during the course in an exercise simulating terrorist threats and attacks against critical infrastructure.

In addition to offering the Critical Infrastructure Protection Against Terrorist Attacks course, the Center of Excellence Defense Against Terrorism signed a Memorandum of Agreement with the US Army War College in 2019 to explore ways in which both entities can help each other in CIP/CISR. Initial joint projects include:

- Publishing a book on CISR focused on what are commonly referred to as the "lifeline infrastructure sectors" – communications, energy, transportation, and water management.
- Developing an online listing of CISR reference materials for use by all NATO and partner nations.
- Developing a 2-day senior seminar on CISR for senior public and private sector officials; and

- Exploring new opportunities to more directly assist Alliance and partner nations in developing CISR policies, plans and procedures, including the recommendation that the Center of Excellence Defense Against Terrorism establish a CISR Mobile Training Team.

NATO has made appreciable progress in protecting critical infrastructure, but the process is extraordinarily complex and a huge continuing challenge - requiring multiple streams of work performed by a wide variety of public and private sector stakeholders. Some of the major steams of work include:

- Identifying and Determining the Criticality of National Infrastructure
- Determining the Terrorist Threat to and Risk to specific Critical Infrastructures
- Determining Critical Infrastructure Vulnerabilities
- Mapping Critical Infrastructure Dependencies and Interdependencies
- Using Applicable Risk Management Approaches
- Developing and Implementing National Critical Infrastructure Protection Policy
- Managing the Response to a Credible Terrorist Threat or Attack Against CI
- Establishing and Implementing Mechanisms for Sharing Information and Intelligence Between Government and CI Owners and Operators
- Developing and Implementing Continuity of Operations/Disaster Recovery Plans for Critical Infrastructure
- Providing Physical and Cyber Protective Measures
- Ensuring the Integrity, Security and Continuity of Critical Infrastructure Supply Chains
- Minimizing Critical System Recovery Times
- Adopting the Principal Concepts of Critical Infrastructure Security and Resilience

The nexus between the CISR and CT communities in every nation is different -- determined primarily by the extent to which the counterterrorism community is actively contributing its knowledge, skill, and ability to support the overarching CISR work streams identified above.

Are there good practices, or international standards in these and other CISR work streams to safeguard CI from terrorist acts?

Best Practices in Protecting CI Against Terrorist Attacks

The title of this chapter is: Best Practices for Strengthening the Protection of NATO and Partner Nation Critical Infrastructure Against Terrorist Attacks: *It is All About the "HOW"*. Before we discuss the "*HOW*", it is important to discuss the "*WHAT*".

The "WHAT"

When thinking initially about "good practices" in the CIP/CISR domain, one probably envisions a somewhat lengthy list of *"WHAT"* a nation, ministry, agency, or specific sector has done in one or more of CISR work streams that has proven to be demonstrably effective in achieving a specific goal or objective.

NATO and other international organizations, such as the European Union and United Nations, have worked with international, regional, and sub-regional organizations to identify and share good practices and measures, and they are committed to fostering targeted capacity development, information sharing, training and exercises, technical assistance, and technology transfer to protect critical infrastructure from terrorist attacks.

In this regard three recently published compendiums/reports of good practices in protecting critical infrastructure against terrorist attacks, which are worthy of attention, include:

- The 2018 Report by the United Nation's Counter-Terrorism Implementation Task Force's Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security titled: *The Protection of Critical Infrastructure Against Terrorist Attacks: A Compendium of Good Practice.* This 182-page report addresses prevention, preparedness, mitigation, investigation, response, recovery and provides excellent reference material from many NATO, EU, and other nations on the development of strategies for reducing risks to critical infrastructure from terrorist attacks.[34]
- The 2019 report by the United States Department of Homeland Security titled: *A Guide to Critical Infrastructure Security and Resilience.* This report contains basic information of U.S. lessons learned over the last 15 years, which may be helpful to other countries, particularly those countries that are considering developing or refining their own voluntary and regulatory-based infrastructure protection/security and resilience programs.[35]
- The 2019 book published under the NATO Science for Peace and Security series titled, *Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection.* This book presents edited contributions from the NATO Advanced Training Course on Critical Infrastructure Protection - Best Practices and Innovative Methods of Protection, which was held in Agadir, Morocco, from 6 to 12 May 2018. This course brought together specialists from Member States and partner nations working around protecting critical infrastructure to share their knowledge and expertise.[36]

Together, these three documents provide scores of best/good practices in protecting CI against terrorist attacks. However, it is the author's belief that it is more important to identify "*HOW*" (the way) nations, ministries, agencies, and specific sectors build sustain a viable, risk-based CIP/CISR posture.

---

[34] United Nations, *The Protection of Critical Infrastructure*.
[35] CISA, *A Guide to Critical Infrastructure Security and Resilience*.
[36] Kruszka et. al. (eds.), *Critical Infrastructure Protection*.

It is All About the "HOW"

Nearly 20 years ago, former Harvard University Professor John P. Kotter wrote a seminal article titled, "What Leaders Really Do" for the Harvard Business Review.[37] In his article, Kotter said: "Leadership and management are two distinctive and complementary systems of action. Each has its own function and characteristic activities. Both are necessary for success in an increasingly complex and volatile business environment. Management is about coping with complexity. Leadership, by contrast, is about coping with change. Management develops the capacity to achieve its plan by organizing and staffing— creating an organizational structure and set of jobs for accomplishing plan requirements, staffing the jobs with qualified individuals, communicating the plan to those people, delegating responsibility for carrying out the plan, and devising systems to monitor implementation. The equivalent leadership activity, however, is aligning people. This means communicating the new direction to those who can create coalitions that understand the vision and are committed to its achievement. Finally, management ensures plan accomplishment by controlling and problem solving—monitoring results versus the plan in some detail, both formally and informally, by means of reports, meetings, and other tools".[38]

As stated earlier in this chapter, the process of building and sustaining CISR is very complex and concerns itself with responding (coping, if you will) to a rapidly changing security environment. Like any complex process, especially in the national security domain, if it is going to be done well, it requires top-notch leadership and management, as defined by Kotter. And after being actively involved in the CIP/CISR community for nearly 30 years, it is my opinion that "*WHAT*" needs to be done (work streams/good practices) is important; but the extent to which a nation develops and implements the "WHAT" is defined by the extent to which those responsible for leading and managing national CIP/CISR programs foster the communication, cooperation, collaboration, coordination, and concentration required to build and sustain a viable, risk-based CIP/CISR posture that:

- Harmonizes CISR work streams.
- Produces economies of scale.
- Optimizes the allocation of financial and human resources.
- Is flexible and adaptable to changing conditions (both foreseeable and unexpected).
- Enables rapid recovery from disruption.
- Establishes a culture of security and resilience; and
- Demonstrably reduces the risks to CI posed by terrorism, or any other threat.

In this regard, there are three overarching "good practices" where communication, cooperation, collaboration, coordination, and concentration are needed the most are:

---

[37] Kotter, *What Leaders Really Do*.
[38] Ibid.

- Adopting a sound approach to CI risk management.
- Developing, managing, and sustaining Public-Private Partnerships between the national government and the owners and operators of CI.
- Establishing mechanisms for sharing CISR information between the national government and owners and operators of CI.

These three good practices have come about due to the critical lessons learned by nations which have been on the leading edge of CIP/CISR planning for many years and have experienced the trials and tribulations associated with building and implementing national CIP/CISR policies that have served as good models for other nations to emulate.

Adopting a Sound Approach to CI Risk Management

Risk management focuses resources on those threats and hazards that are most likely to cause significant, unwanted outcomes to a specific infrastructure or sector and informs actions designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration. Risk management facilitates decision making and the setting of priorities across all stakeholders. A risk management framework sets out an approach to consistently:

- Identify, analyze, and allocate resources to deter, detect, disrupt, and prepare for threats and hazards to critical infrastructure.
- Prioritize vulnerability reduction efforts, address physical features or operational attributes that make an infrastructure element open to exploitation or susceptible to a given hazard; and
- Mitigate the potential consequences of incidents proactively or prepare to mitigate them effectively if they do occur.[39]

The risk management framework can be applicable to all levels of government or private sector organizations. It should cover all threats and hazards and varying factors across critical infrastructure sectors, in addition to individual assets and systems. Many models/methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the allocation of resources to reduce those risks.

How risk assessment, analysis and management are performed is a critical aspect of CIP/CISR. Implementing a risk-based prioritization of resources — whether at the facility, community, or other level — it requires information about the threats, vulnerabilities, and consequences of a variety of potential scenarios. To form a basic strategy for reducing the risk from terrorist attacks, decision-makers need (1) evidence-based threat assessments to provide comparative analysis of a range of adversaries and attack methods, and (2) imagination-based analysis to give them alternate perspectives on the threats they face, including information on the ways that the terrorist threat may change.[40]

[39] CISA, *A Guide to Critical Infrastructure*.
[40] French, *Intelligence Analysis.*

An evidence-based risk analysis system that can illustrate capability levels for a series of attack methods and the related intent levels for classes of targets and geographic regions would enable risk management across a sector, in a city or region, and at the facility or system level. It would also provide useful distinctions among the threat for scenarios that combine the attacker, a method of attack, and the attack's target.

Evidence-based systems alone cannot provide all the insight that decision-makers need to consider threats. Their value is that they can show how the weight of evidence influences judgments about the severity of a threat. Their weakness is that the dependence on past events and clear indications of capability or intent will prevent them from providing timely insight into sudden or more radical shifts in the threat that require more innovative approaches to identify. Imagination-based analysis frees an analyst from the constraints of a structured model and complements the insight that evidence-based systems provide. Red Cell analysis, Red Team exercises, and game theory are three established approaches to this less structured area of threat analysis.

Although imagination-based analysis can inform the decision-making process, it is a challenge for decision-makers to use it as a basis for investments or action. Even the best imaginative work carries a high degree of uncertainty. Risk management must begin with a strategic, evidence-based threat analysis.[41]

Information about vulnerabilities and consequences can often be obtained from the owner or operators of key facilities or from an outside expert. All-inclusive information on the terrorist threat, however, can only come from the national government. Members of the critical infrastructure protection community — sub-national governments, owners and operators, and national ministries or agencies with security responsibilities — need to be specific in their requests for threat analysis.[42]

Risk assessments give decision makers better information to determine which mitigation and risk management measures are most critical and to understand where distinct types of actions are most suitable. The range of available measures includes coordination with other stakeholders; provision of additional response or recovery equipment; modifications to infrastructure design; restrictions on operations; and hiring and training of staff, among others. Risk assessments also keep the focus from automatically defaulting to rare or worst-case events with extreme consequences, promoting consideration of a range of more likely events, even if they have lesser, but still significant, consequences.[43]

The European Commission Joint Research Centre Institute for the Protection and Security of the Citizen published a report called, "Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art" which provides an overview of 21 risk assessment methodologies developed and used by several nations worldwide.[44]

---

41 Ibid.
42 Ibid.
43 CISA, *A Guide to Critical Infrastructure*.
44 Giannopolous et. al., *Risk Assessment Methodologies for Critical Infrastructure Protection*.

Developing, Managing, and Sustaining Public-Private Partnerships

Ensuring the security and resilience of the nation's critical infrastructure is a shared responsibility among multiple stakeholders because neither the government nor the private sector alone has the knowledge, authority, or resources to accomplish CISR alone. The private sector owns and operates a vast majority of the nation's critical infrastructure, so partnerships between the public and private sectors that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience.

Broad-based participation is key to the successful development and implementation of a comprehensive program to promote continuous improvement in security and resilience. Identifying the roles and responsibilities of different stakeholders at the beginning can help align and even combine relevant expertise/disciplines, focus efforts, ensure that timelines are met, and provide the desired inputs for an effective program. Similarly, identifying existing programs or efforts that relate to infrastructure security and resilience can help anchor the development of an overall program and serve as a guide to other sectors.

Public-Private Partnerships involve integrated interactions among public and private sectors, structured around agreed-upon performance standards that guide desired CIP/CISR outcomes. CIP/CISR Public-Private Partnership formation and engagement enhances communication, planning, risk assessment, program implementation, and operational activities, including incident response and recovery. Mistrust, unaligned goals, diverging strategies, unfair risk accumulation on few partners or inefficient distribution of responsibilities can result in failure of the public/private partnership.[45]

Establishing Mechanisms for Sharing CISR Information

Successful information sharing requires established mechanisms or channels (often developed and managed through Public-Private Partnerships) to reach CISR stakeholders regularly, as well as before, during, and after an incident. Sharing information can take many forms, including training events, briefings, email alerts, conference calls, or meetings in secure locations to discuss classified materials about specific threats or hazards, and documents and forums that encourage sharing lessons learned. The latter category improves the planning for handling future events.[46]

The followings can help facilitate and support information sharing efforts:

- Identify stakeholders who have an interest and/or stake in critical infrastructure security and resilience.
- Provide actionable threat information so that owners/operators can implement plans and take appropriate action.
- Recognize that information sharing must be reciprocal – as owners and operators may each observe suspicious activity that helps identify and validate threats.

[45] Geis and Schulz, *Critical Infrastructure*.
[46] CISA, *A Guide to Critical Infrastructure*.

- Establish and maintain user-friendly information sharing systems for stakeholders to promote routine as well as rapid communication during events/emergencies.
- Threat information should be processed to remove the specifics of data sources and collection methods, so it can be shared more broadly, particularly with relevant stakeholders.
- Owner and operator information must be protected, in accordance with national legislation.

Information-sharing should be provided in a way that allows informed action on three levels:

- Situational awareness in both normal, day-to-day operations and a crisis or event, including suspicious activity reporting, incident analysis, and recommended protective actions.
- Operational and tactical risk management actions in anticipation of and response to a threat to critical infrastructure at a specific location or across an entire sector.
- Strategic planning and investment to build capabilities that strengthen critical infrastructure security and resilience for the future.

Information shared within a structured and secure information sharing environment helps critical infrastructure owners and operators guide investments, implement protective programs, and ensure effective response to infrastructure threats as they arise. Information being shared should be accurate, relevant, timely, and actionable. To be most effective, information sharing must be multidirectional. Threat information from the national government, when applicable, should be shared with critical infrastructure partners at the appropriate classification level, and as much as possible at the unclassified level.

The risks associated with information sharing and safeguarding are reduced through the adoption of sound policies and standards. Building trust in sharing and safeguarding requires the ability to manage risk. Risk to national security increases when the approach to information sharing is inconsistent, fragmented, or managed from a single-agency perspective. Risk decreases with sound policies and standards, increased awareness and comprehensive training, effective governance, and enhanced accountability.

Conclusion

NATO is actively pursuing CIP/CISR across the Alliance and with partner nations. While CISR is a continuing global challenge, it will also be an increasingly significant issue of concern in the years ahead. Extraordinary levels of domestic, regional, and international communication, coordination, cooperation, collaboration, and concentration will be required to secure improved levels of CIP/CISR. Continuous but expensive organizational learning will also be essential to producing an auto adaptive CISR posture for dealing more effectively with adaptive predators and dynamic uncertainty.

The last two decades have taught us that there are three overarching "good practices" (Sound Risk Management, Public-Private Partnership, and Information Sharing) which comprise the foundation upon which all other CISR efforts are built. These three good practices will determine, ultimately, the extent to which any nation achieves defined success in any CIP/CISR endeavor. And make no mistake about it, a nation's counterterrorism organization (or community of organizations) should be contributing its expertise to any work stream concerned with the terrorist threat. There are clear and present risks to CI, but sound risk management requires imagining the future as well as defining the present.

NATO can further strengthen its contribution to Alliance and partner nations by establishing a comprehensive system of CISR indicators (Resilience Monitor/Index), beyond those seven currently being used by Civil Emergency Planning. It should also foster increased engagement between all elements engaged in, or planning to engage in, CIP/CISR activities, particularly in the areas of training and education. In this regard NATO should fully support plans by the Center of Excellence Defense Against Terrorism to expand its CISR curriculum and joint projects with the US Army War College. NATO should also support the establishment of a CISR Mobile Training Team capability at the Center of Excellence Defense Against Terrorism to work directly with partner nations to develop strategies for addressing partner--identified gaps in CIP/CISR. And lastly, NATO should stress the vital need for Alliance and partner nations to focus intently on implementing the three fundamental building blocks of CIP/CISR -- sound risk management, public-private partnerships and information sharing.

Bibliography

Auerswald, Philip, Branscomb, Lewis, La Porte, Todd M., and Michel-Kerjan, Erwann, (2005), "The Challenge of Protecting Critical Infrastructure ", *Issues in Science and Technology*, Vol. 22, No. 1, Fall 2005, https://issues.org/auerswald/. (Accessed 15 December 2020)

Clemente, Dave, (2013), "Cyber Security and Global Interdependence: What is Critical?", *Chatham House*, February 2013, https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf. (Accessed 15 December 2020)

Council of Europe, "Budapest Convention and Related Standards", https://www.coe.int/en/web/cybercrime/the-budapest-convention. (Accessed 15 December 2020)

Domestic Preparedness, (2013), "Presidential Policy Directive (PPD-21) - Critical Infrastructure Security & Resilience", 20 February 2013, https://www.domesticpreparedness.com/updates/presidential-policy-directive-ppd-21-critical-infrastructure-security-resilience/. (Accessed 15 December 2020)

EUR-Lex, "Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism", https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52004DC0702. (Accessed 15 December 2020)

European Commission, "Critical Infrastructure", https://ec.europa.eu/home-affairs/e-library/glossary/critical-infrastructure_en. (Accessed 15 December 2020)

European Commission, "Protection", https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en. (Accessed 15 December 2020)

Fausboll, Carsten, "NATO Civil Emergency Planning (CEP)", https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OSN/Documents/04_NATOCivilEmergencyPlanning1.pdf. (Accessed 15 December 2020)

French, Geoffrey S., (2007), "Intelligence Analysis for Strategic Risk Assessments", in *Critical Infrastructure Protection: Elements of Risk,* (George Mason University), https://cip.gmu.edu/wp-content/uploads/2016/06/ElementsofRiskMonograph.pdf. (Accessed 15 December 2020)

Geis, Isabella and Schulz, Wolfgang H., (2015), "Critical Infrastructure: Making it Private or Public – An Institutional Economic Discussion on the Example of Transport Infrastructure". *Conference Paper,* presented at 2015 Annual Meeting of the Midwest Political Science Association, 16-19 April 2015.

Giannopolous, Georgios, Filippini, Roberto, and Schimmer, Muriel, (2012), "Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art", *JCR European Commission,* https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf. (Accessed 15 December 2020)

https://www.un.org/counterterrorism/ctitf/en/protection-critical-infrastructure-including-vulnerable-targets-internet-and-tourism-security

INTERPOL, (2020), "Focus: Interpol Major Events Support Teams", 31 January 2020, https://www.interpol.int/News-and-Events/News/2020/Focus-INTERPOL-Major-Events-Support-Teams. (Accessed 15 December 2020)

Jahier, Khan, (2014), "Critical Infrastructure Protection within NATO", *CIPRE-EXPO*, February 2014, https://www.cipre-expo.com/wp-content/uploads/2014/02/Khan-Jahier-NATO-CIP-within-NATO.pdf. (Accessed 15 December 2020)

Johnathan Tal, "America's Critical Infrastructure: Threats, Vulnerabilities and Solutions", *Security Infowatch,* 20 September 2018, https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions. (Accessed 15 December 2020)

Kotter, John P., (2001), "What Leaders Really Do", *Harvard Business Review*, December 2001, https://enterprisersproject.com/sites/default/files/What%20Leaders%20Really%20Do.pdf. (Accessed 15 December 2020)

Kruszka, Leopold, Klósak, Maciej, and Muzolf, Paweł (eds.), (2019), *Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection,* (Amsterdam: IOS Press), E-Book, http://ebooks.iospress.nl/volume/critical-infrastructure-protection-best-practices-and-innovative-methods-of-protection. (Accessed 15 December 2020)

National Association of Counties, (2014), "Improving Lifelines: Protecting Critical Infrastructure for Resilient Countries", November 2014, https://www.naco.org/sites/default/files/documents/NACo_ResilientCounties_Lifelines_Nov2014.pdf. (Accessed 15 December 2020)

National Council on Information Sharing and Analysis Centers (ISACs), "ISACs", http://www.nationalisacs.org/. (Accessed 15 December 2020)

NATO HQ, (1997), "Chapter 11: Civil Emergency Planning", October 1997, https://www.nato.int/docu/logi-en/1997/lo-1106.htm. (Accessed 15 December 2020)

NATO HQ, (2016), "Commitment to enhance resilience", 08 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en. (Accessed 15 December 2020)

NATO HQ, (2019), "COE Catalogue", Allied Command Transformation, https://www.act.nato.int/images/stories/structure/coe_catalogue_20190118.pdf. (Accessed 15 December 2020)

NATO HQ, (2019), "Relations with the United Nations", 15 February 2019, https://www.nato.int/cps/en/natohq/topics_50321.htm. (Accessed 15 December 2020)

NATO HQ, (2020), "Civil preparedness", 27 October 2020, https://www.nato.int/cps/en/natohq/topics_49158.htm. (Accessed 15 December 2020)

Niglia, Alessandro (ed.), (2016), "Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges", NATO Science for Peace and Security Series, Vol. 46. Organization of American States (OAS), "Tourism Security Program", http://www.oas.org/en/sms/cicte/prog-tourism-security.asp. (Accessed 15 December 2020)

OSCE, "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", http://www.osce.org/secretariat/103954?download=true. (Accessed 15 December 2020)

Rühle, Michael, (2011), "NATO and energy security", *NATO HQ,* 08 February 2011, http://www.nato.int/docu/review/2011/climate-action/energy_security/EN/index.htm. (Accessed 15 December 2020)

Setola, Roberto, Luiijf, Eric, and Theocharidou, Marianthi, (2016), "Critical Infrastructures, Protection and Resilience", in Roberto Setola *et. al.* (eds.) *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*, (Cham: Springer).

U.S. Department of Homeland Security, Cyber Security & Infrastructure Agency (CISA), (2019), "A Guide to Critical Infrastructure Security and Resilience", November 2019, https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf. (Accessed 15 December 2020)

United Nations General Assembly, (2015), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/174. (Accessed 15 December 2020)

United Nations, (2018), "The Protection of critical infrastructure against terrorist attacks: Compendium of good practices", Counter-Terrorism Committee Executive Directorate (CTED) and UN Office of Counter-Terrorism (UNOCT), https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf. (Accessed 15 December 2020)

United Nations, (2018), "The Protection of critical infrastructure against terrorist attacks: Compendium of good practices", United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter-Terrorism (UNOCT), https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf. (Accessed 15 December 2020)

CHAPTER VI

COUNTERING WMD TERRORISM BEST PRACTICES FOR SAFEGUARDING THE CBRN MATERIAL

Mustafa Kibaroglu

Introduction

Any discussion on countering Weapons of Mass Destruction (WMD) terrorism must start by addressing a fundamental question: Is WMD terrorism just hype or reality? This issue has been an increasingly serious bone of contention amongst scholars and experts in the field of terrorism studies over the past decades.[1] One group argues that the threat of use of WMD in terrorist attacks is exaggerated, pointing to the barriers that exist that cannot be overcome by terrorists in their attempts to gain access to or to develop nuclear, chemical or biological weapons. They also remind us that there has not been a major incident to date where terrorists have made use of WMD in their attacks.[2] On the other hand, there are those who believe that the threat is real, and who emphasize that the absence of use of WMD by terrorists thus far does not mean that they have not attempted to acquire or to use chemical, biological, radiological or nuclear (CBRN) material in their attacks.[3] They remind us that

[1] Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, (New York: Times Books, Henry Hold & Company, 2004); Andrew Blum, Victor Asal, Jonathan Wilkenfeld, John Steinbruner, Gary Ackerman, Ted Robert Gurr, Michael Stohl, Jerrold M. Post, Joshua Sinai, Gary LaFree, Laura Dugan, Derrick Franke, Bartosz H. Stanislawski, Gabriel Sheffer, Mark Irving Lichbach, Todd Sandler, and Walter Enders, "Nonstate Actors, Terrorism, and Weapons of Mass Destruction", *International Studies Review*, Vol. 7, No. 1, March 2005, pp. 133-170; Anne Stenersen, *Al-Qaida's Quest for Weapons of Mass Destruction: The History behind the Hype*, (Riga: VDM Verlag Dr. Müller, 2008); Bruce Hoffman, "CBRN Terrorism Post 9/11", in Russell D. Howard and James Forest (eds.), *Weapons of Mass Destruction Terrorism*, (New York: McGraw Hill, 2007), pp. 264-279; Jonathan B. Tucker (ed.), *Toxic Terror, Assessing Terrorist Use of Chemical and Biological Weapons*, (Cambridge: MIT Press, 2000); Brad Roberts (ed.), *Hype or Reality? The "New Terrorism" and Mass Casualty Attacks*, (Alexandria: The Chemical and Biological Arms Control Institute, 2000); Charles Daniel Ferguson and Michelle M. Smith, "Assessing Radiological Weapons: Attack Methods and Estimated Effects," *Defence Against Terrorism Review*, Vol. 2, No. 2, Fall 2009, pp. 15-34; James Forest, "Framework for Analyzing the Future Threat of WMD Terrorism," *Journal of Strategic Security,* Vol. 5, No. 4, 2012, pp. 51-68; Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" *Belfer Center for Science and International Affairs,* January 2010, https://www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality. (Accessed 15 December 2020)

[2] Peter Zimmerman, "Do We Really Need to Worry? Some Reflections on the Threat of Nuclear Terrorism", *Defence Against Terrorism Review,* Vol. 2, No. 2, Fall 2009, pp. 1-14; Sammy Salama and Lydia Hansell, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *The Nonproliferation Review,* Vol. 12, No. 3, 2005, pp. 615-653.

[3] Gary Ackerman and Michelle Jacome, "WMD Terrorism: The Once and Future Threat", *PRISM*, Vol. 7, No. 3, 18 May 2018, pp. 23-36, https://cco.ndu.edu/Portals/96/Documents/prism/prism7_3/180515_Ackerman_PCP.pdf?ver=2018-05-18-174850-983. (Accessed 15 December 2020)

CBRN material are more accessible, especially since the collapse of the Soviet Union, which used to possess the world's largest weapons arsenal, and which has become the target of terrorist groups and illegal traffickers pursuing WMD capability.[4] Proponents of this view also point to the fact that the profile of terrorist organizations changes and that they could recruit "scientists" and "experts", perhaps by appealing to their religious beliefs as a means to exploit those individuals as opportunities, for example.[5]

Against this background, there are reasons to be both optimistic as well as pessimistic regarding the threat of WMD terrorism and the effectiveness of the counter-measures that can be taken by states and international organizations. On the optimistic side, it is widely believed by experts that producing sophisticated nuclear, biological, or chemical weapons that would meet military standards is beyond the capability of terrorist organizations.[6] Each of these weapons categories requires high levels of technological capability and sophisticated scientific knowledge. These could normally only be brought together systematically with the specific objective of manufacturing such weapons by way of financing large-scale projects under the auspices of the state enterprises or huge private corporations operating in the defense industry. Hence, it would make sense to argue that, for the foreseeable future, terrorist organizations are not likely to have the capacity to manufacture WMD of their own.

But, on the other hand, there are reasons to be quite pessimistic. Terrorists do not necessarily need to produce WMD themselves to achieve their goals. They may be satisfied with the extent of the damage and, more importantly, the fear that their attack would cause in public by using "crude weapons" or "dirty bombs" made of CBRN material.[7] Terrorists would need only to smuggle some 50 kilograms of highly enriched uranium (HEU), an amount that would fit into six one-liter milk cartons, across borders to create an improvised nuclear device that could level a medium-sized city. Border controls currently do not provide adequate defense against this threat.[8] Moreover, the means and methods that terrorists might use in their attacks may not necessarily require a high degree of sophistication. Simple machinery or techniques, such as agricultural sprayers, ventilators, or civilian aircraft might

---

4 John M. Shields and William C. Potter (eds.), *Dismantling the Cold War: U.S. and NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program*, (Cambridge: The MIT Press, 1997).

5 Reshmi Kazi, "The Correlation Between Non-State Actors and Weapons of Mass Destruction, *Connections*, Vol. 10, No. 4, 2011, pp. 1-10.

6 Experts state that the production of sophisticated devices should not be considered to be a possible activity for a fly-by-night terrorist group. It is, however, conceivable in the context of a nationally supported program able to provide the necessary resources and facilities and an established working place over the time required. Carson Mark, Theodore Taylor, Eugene Eyster, William Maraman, and Jacob Wechsler, "Can Terrorists Build Nuclear Weapons*?" Nuclear Control Institute,* 2002, https://www.nci.org/k-m/makeab.htm. (Accessed 15 December 2020)

7 Many analysts believe that this type of weapon, which could disperse radioactive materials across a wide area, might be particularly attractive to terrorists. If a radiological dispersal device (RDD) would be used, radioactive material, which is composed of atoms that decay, emitting radiation, might cause serious harm to human health. Jonathan E. Medalia, "'Dirty Bombs': Technical Background, Attack Prevention and Response, Issues for Congress"*, Congressional Research Service,* Report No. R41891, 24 June 2011, https://fas.org/sgp/crs/nuke/R41890.pdf. (Accessed 15 December 2020)

8 United Nations General Assembly, A More Secured World: Our Shared Responsibility: Report of the High-level Panel on Threats, Challenges and Change, A/59/565, 02 December 2004, p. 21, https://www.un.org/ruleoflaw/files/gaA.59.565_En.pdf. (Accessed 15 December 2020)

suffice for dispersing chemical or biological agents.[9] Hence, metropoles and other residential areas are vulnerable to terrorist attacks due to the low level of security checks. Alternatively, industrial facilities, critical infrastructure, harbors or airports may be the primary targets.[10] In any of these incidents, should they ever occur, the consequences would be devastating in many respects. While the number of fatalities would depend on the degree of destructive power that the method of attack involves, the substances used in the attack could intoxicate or poison people in the immediate surrounds of the location of the incident, and pollute the environment affecting all life forms in the wider area, as well.[11]

One sure way to eliminate the likelihood of terrorism with WMD would be to eliminate all nuclear, chemical and biological weapons in the world. But this is hardly possible due to the existence of nuclear weapons in the arsenals of nine states;[12] the large stocks of fissile material coming from the weapons dismantlement programs as a result of the disarmament agreements between the United States and Russia; the hundreds of nuclear power and research reactors that are in operation or under construction in dozens of countries around the world;[13] the hundreds of tons of declared chemical weapons that have yet to be destroyed;[14] and the lack of clarity about the status of biological research and development programs in various countries due to the absence of a verification mechanism of the Biological Weapons Convention.[15] It is, therefore, crucial that WMD and CBRN material are kept in safe and secure places, away from the reach of terrorists.[16] This, however, requires a major commitment of the responsible civil and military authorities to the safety and security of every single facility in every country around the world where WMD and/or CBRN material have been developed, produced, or stockpiled.

---

9 Author's notes from the presentation of David R. Franz from Southern Research Institute, Frederick, MD, during the NATO Advanced Research Workshop on "The Role of Biotechnology in Countering BTW Agents," convened in Prague, Czech Republic on 21-23 October 1998.

10 Selcuk Cankaya and Mustafa Kibaroglu (eds.), *Bioterrorism: Threats and Deterrents,* (Amsterdam: IOS Press, 2010).

11 Dan Radu Voica and Mustafa Kibaroglu (eds.), *Responses to Nuclear and Radiological Terrorism*, (Amsterdam: IOS Press, 2011).

12 United States, Russia, United Kingdom, France, China, Israel, India, Pakistan, and North Korea.

13 The International Atomic Energy Agency (IAEA) lists on its website 220 operational nuclear research reactors in 53 countries (IAEA, "Research Reactor Database, https://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx?filter=0. Date of Access: 15 December 2020) and 442 power reactors in 30 countries (IAEA, "The Database on Nuclear Power Reactors", https://pris.iaea.org/PRIS/home.aspx. (Accessed 15 December 2020)

14 It is stated on the website of the Organization for the Prohibition of Chemical Weapons (OPCW), the implementing body for the Chemical Weapons Convention, that out of the 72,304 metric tons of the total declared stockpiles of chemical agents in the world, by 31 October 2020, 71,123 metric tons (meaning 98.37 percent of the world's declared chemical weapons stockpiles have been destroyed. This figure also means that there exist 1,181 metric tons of declared stockpiles of chemical agents yet to be destroyed. OPCW, "OPCW by the Numbers", https://www.opcw.org/media-centre/opcw-numbers. (Accessed 15 December 2020)

15 Filippa Lentzos*, Compliance and Enforcement in the Biological Weapons Regime*, WMD Compliance & Enforcement Series, Paper Four, United Nations Institute for Disarmament Research (UNIDIR), 2019, https://www.unidir.org/sites/default/files/2020-02/compliance-bio-weapons.pdf (Accessed 13 April 2021)

16 Matthew Bunn, William H. Tobey, Martin B. Malin, and Nickolas Roth, "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?", *Belfer Center for Science and International Affairs*, Project on Managing the Atom, March 2016, https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf. (Accessed 15 December 2020)

Bearing this in mind, this chapter contends that the threat of WMD terrorism is credible and real, and maintains that, in order to counter the threat, states and the concerned international organizations must assign the utmost priority to preventing terrorist organizations from having access to nuclear, chemical, and biological weapons, as well as the material, technology and know-how that are necessary for their manufacture. Therefore, the chapter highlights a set of multilateral measures that have been initiated by states, either individually or in collaboration with other states, extending from the Cooperative Threat Reduction (*"Nunn-Lugar"*) Program, and the Proliferation Security Initiative, to the United Nations Security Council Resolution 1540, and the Nuclear Security Summits. The sections below briefly discuss each of these four initiatives for countering WMD terrorism as the good practices of comprehensive political and legal processes as well as elaborate scientific and technological mechanisms that have been developed over the years with a view to effectively safeguarding and securing CBRN material around the world. The chapter also presents the Turkish experience in this context as a case where the good practices and the lessons learned from the aforementioned, ground-breaking initiatives that have been widely adopted in devising as well as implementing the export control regime of Turkey.

Good Practices for Safeguarding the CBRN Material

It goes without saying that, for countering WMD terrorism, preventing the access of terrorist groups to CBRN material and disrupting the terrorist networks that are involved in their illicit trafficking is crucial. These efforts, however, require effective and extensive inter-agency cooperation both within the state apparatus as well as between states.[17] To achieve this objective, the following multilateral efforts have been put in place with the effective and sustained contribution of many states and international organizations in order to mobilize concerted action against the sources of the threat.[18]

Cooperative Threat Reduction Program

A very important step in this direction, and the first good practice discussed in this chapter, is the Cooperative Threat Reduction (CTR) Program, also known as the "Nunn-Lugar Program" after the two U.S. Senators, Sam Nunn (Dem, GA) and Richard Lugar (Rep, IN) who initiated the bill at the U.S. Congress in the aftermath of the Cold War in 1991. The purpose of the CTR program was to help the former Soviet republics to destroy nuclear weapons, chemical weapons, and other weapons, to transport, store, disable, and safeguard weapons in connection with their destruction, and to establish verifiable safeguards against the proliferation of such weapons to reduce the chances of the material used in their manufacture falling into the hands of terrorist groups or some states of concern. As such,

[17] Mustafa Kibaroglu, "The Threat of Nuclear Terrorism Requires Concerted Action" *Strategic Analysis*, Vol. 38, No. 2, March 2014, pp. 209-216.

[18] Osman Aytac and Mustafa Kibaroglu (eds.), *Defense Against Weapons of Mass Destruction Terrorism*, (Amsterdam: IOS Press, 2009).

beyond WMD elimination, CTR programs established a professional "contractor culture" in Russia that is still functioning today.[19] Thus, Nunn-Lugar has been one particular domain of intensive cooperation and collaboration between the United States and Russia that was not negatively affected by the deterioration of relations between the two states in the post-Cold War era.

At the time of the CTR program's establishment in late 1991, the Soviet Union's nuclear arsenal was estimated at well over 10,000 strategic nuclear warheads, as well as up to triple that amount of tactical nuclear weapons, and which were deployed in Belarus, Kazakhstan, and Ukraine in addition to Russia. Early projects included purchases of armored blankets, storage containers, railcar improvements, and emergency response vehicles for nuclear warhead security. As thousands of nuclear warheads were dismantled, CTR support has also focused on the safe storage of bomb-grade fissile materials (HEU and Plutonium). A major effort since the mid-1990s has been the construction of a storage facility at Mayak, outside of Chelyabinsk, worth 400 million USD, and designed to hold more than 25,000 fissile material containers from approximately the same number of nuclear warheads. In addition to the security, transportation, and storage of nuclear warheads and bomb-grade fissile materials, the dismantlement and destruction of nuclear weapons systems have been major CTR tasks and have helped in the implementation the 1991 Strategic Arms Reduction Treaty (START) and the 2002 Strategic Offensive Reductions Treaty. The CTR program can claim a long list of accomplishments in reducing the amount of availability of former Soviet weaponry. Perhaps most important, all nuclear warheads have been returned to Russia from the former Soviet republics of Belarus, Kazakhstan and Ukraine and all strategic weapons infrastructure, including missiles and silos, have been eliminated as well.[20]

The safe storage or destruction of Russian chemical weapons has also been a top priority of the CTR program. Russia signed the Chemical Weapons Convention in 1993 and declared seven chemical weapons stockpiles containing a total of 40,000 metric tons of nerve and blister agents. The United States, after a July 1994 inspection of the chemical weapons destruction site at Shchuch'ye, decided to help Russia build a large demilitarization facility at the 5,400-ton nerve agent stockpile. This stockpile was chosen primarily because of its proximity to the southern Russian border and the portability of its two million artillery shells. The CTR program has committed more than 1.1 billion USD for this effort, including the provision of mobile testing laboratories, the construction of a Central Analytical Lab in Moscow, and the dismantlement of two former chemical-agent production facilities. Russia announced its completion of the destruction of all declared chemical agents in October 2017. Yet the neutralization process left tens of thousands of tons of toxic liquid. Russia was incinerating some of this liquid at sites and had also decided to solidify the liquid produced at Shchuch'ye

[19] Congressional Research Service, "The Evolution of Cooperative Threat Reduction: Issues for Congress", Report R43143, 23 November 2015, p. 5, https://fas.org/sgp/crs/nuke/R43143.pdf. (Accessed 15 December 2020)

[20] Paul Walker, "Nunn-Lugar at 15: No Time to Relax Global Threat Reduction Efforts", *Arms Control Today*, May 2006, https://www.armscontrol.org/act/2006-05/features/nunn-lugar-15-time-relax-global-threat-reduction-efforts. (Accessed 15 December 2020)

with bitumen and store it in sealed, retrievable bunkers, planning to treat the neutralized mustard agent at Gorny and Kambarka and retrieve arsenic for later industrial use. This was a major accomplishment for Russia and achieved partly due to 2-3 billion USD funding from the CTR program. Similarly, in 2007, at the request of the Albanian government to the OPCW, the CTR program helped to secure and to destroy a stockpile of 16 tons of mustard agent in storage containers found in a small garage in the mountains outside of Tirana.[21]

The Soviet Union also had a substantial biological weapons research and production program, both military and also under the ostensibly civilian Biopreparat. CTR helped improve safety and security at some of Russia's deteriorating Biopreparat research sites and facilitated the elimination of infrastructure and equipment at biological research and production centers that had the capability to produce biological weapons, including the Stepnogorsk Scientific Experimental and Production Base in Kazakhstan, a biological warfare production complex.[22] This cooperation with Kazakhstan led to similar projects aimed at reducing risks and enhancing the safety and security at other Biopreparat facilities that stored pathogens capable of being weaponized. The program also improved disease detection and surveillance capabilities in several countries of the former Soviet Union.[23] Biologically focused CTR activities have now expanded globally—primarily with support from the U.S. Department of Defense Biological Threat Reduction Program, and the Department of State Biosecurity Engagement Program—to include projects at civilian facilities to prevent theft and diversion of dangerous pathogens and to improve biosecurity, biosafety, and bio-surveillance.[24]

Funding for the CTR program came initially from the US Department of Defense, but over time the State Department and the Department of Energy provided expertise and funding for CTR-related activities in the former Soviet Union and, later, in other regions. The Department of Defense alone spent nearly 7 billion USD on CTR programs between 1991 and 2013, contributing to the deactivation of more than 13,300 former Soviet nuclear warheads; the destruction or elimination of over 3,880 launchers, delivery systems, and platforms including ICBMs,[25] SLBMs,[26] and long-range bomber aircraft; the sealing of 194 nuclear test tunnels; and the destruction of nearly 40,000 metric tons of declared chemical weapons.[27]

Demilitarization programs helped re-orientate former Soviet scientists and military infrastructure from military efforts to peaceful purposes. One such effort included the establishment in 1992 by the United States, Japan, the European Union (EU), and Russia of the

[21] *Ibid*.

[22] Lynn Rusten, Richard Johnson, Steve Andreasen and Hayley Anne Severance, "Building Security Through Cooperation", *Nuclear Threat Initiative*, 2019, pp. 20-21, https://media.nti.org/pdfs/NTI_DPRK2019_RPT_FNL.pdf. (Accessed 15 December 2020)

[23] Joseph P. Harahan, *With Courage and Persistence: Eliminating and Securing Weapons of Mass Destruction with the Nunn-Lugar Cooperative Threat Reduction Programs*, (Washington D.C.: Defense Threat Reduction Agency, 2014), https://www.dtra.mil/Portals/61/Documents/History/With%20Courage%20and%20Persistence%20CTR.pdf?ver=2016-05-09-102902-893. (Accessed 15 December 2020)

[24] Paul Walker, "Nunn-Lugar at 15: No Time to Relax Global Threat Reduction Efforts", (2006).

[25] Inter-Continental Ballistic Missile.

[26] Submarine-Launched Ballistic Missile.

[27] Defense Threat Reduction Agency, "Nunn-Lugar CTR Scorecard," May 2013, https://www.dtra.mil/Portals/61/Documents/20130501_fy13_ctr-scorecard_slides_may13.pdf. (Accessed 15 December 2020)

International Science and Technology Center in Moscow, which provided grants to Russian scientists and supported cooperative research. Several other former Soviet countries joined the Moscow-based center, and other nations, including Norway and the Republic of Korea, became donor countries. A similar center was established in Ukraine in 1993, with additional participating and donor countries. The Moscow center was relocated to Kazakhstan in 2015 after Russia withdrew from participation in 2013. Nearly 40 countries currently participate in these centers, which have funded projects to employ scientists, including some who had been involved with or have expertise relevant to nuclear, biological, and chemical weapons and could, in the absence of adequate employment, be tempted to share their knowledge with other countries or with terrorist organizations.[28]

The terrorist attacks of 11 September 2001 heightened global fears of terrorist groups acquiring WMD and weapons-usable materials. After CTR's success in the former Soviet Union, the George W. Bush administration successfully applied the CTR framework to secure nuclear and radiological materials globally and to prevent their proliferation to countries including in the Middle East and Asia with active terrorist organizations. The Obama administration further expanded CTR's global application to assist with both non-proliferation and counterterrorism efforts. This reflected the post-9/11 expansion of CTR beyond the former Soviet Union, as well as the expiration of the bilateral umbrella agreement governing CTR cooperation between the United States and Russia in 2012, and the fact that Russia no longer wanted the sort of assistance that had been provided since the 1990s. By the same token, CTR funding was essential to activities beyond Russia, including the U.S. contribution to the cooperative effort with Russia and other countries to eliminate Syria's declared chemical weapons stockpile in 2013–2014.[29]

The successes of the CTR program served as a model and a beacon for other nations. In the 1990s, countries including Canada and Germany provided CTR like assistance directly to the former Soviet Union or contributed support to U.S. efforts. In the 2000s, U.S. authorizing legislation for CTR programs in the Department of Defense and the Department of Energy was amended to permit the receipt of funds from other nations to the U.S. Treasury as direct contributions to those programs. Following the September 11 attacks, the United States appealed to other countries to increase resources to help prevent a terrorist attack using WMD. This effort led to additional countries contributing to threat reduction work in the former Soviet Union and later in other regions. Under Canada's leadership, at the July 2002 Group of Eight (G-8) Summit in Kananaskis, Canada, the G-8 countries[30] issued a statement outlining a new initiative entitled "The G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction" as a long-term program to stop the spread of WMD and related materials and technology. The G-8 Global Partnership committed to a "10

---

[28] Lynn Rusten, *et. al*., p. 20.

[29] Mary Beth Nikitin and Amy F. Woolf, "The Evolution of Cooperative Threat Reduction: Issues for Congress", *Congressional Research Service*, CRS Report No. R43143, November 2015, https://fas.org/sgp/crs/nuke/R43143.pdf. (Accessed 15 December 2020)

[30] The G-8 consisted of the G-7 major industrial countries: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, plus Russia.

plus 10 over 10" formula[31] to fund non-proliferation projects, initially in Russia and the former Soviet Union but increasingly to other regions. The Global Partnership was renewed in 2011 with at least 27 countries participating as donor nations.[32] Each nation allocates its funds to those projects it views as a high priority. The donor countries share common implementation principles, project ideas, and experiences, and they monitor progress via working groups and meetings. The programs are executed globally and include nuclear security, disposal of fissile materials, chemical weapons elimination, and biosecurity.[33]

Proliferation Security Initiative

Critical norms and constraints against the proliferation of WMD, which most states honor, have been insufficient to counter the actions and ambitions of some states, terrorist groups and corrupt proliferators who reject, and are determined to violate, those established international norms. New and innovative approaches were, therefore, necessary to combat proliferation in the 21st Century.[34] Hence, a series of developments have paved the way for the establishment of the Proliferation Security Initiative (PSI), which is discussed here as the second good practice in countering WMD terrorism.

On 11 December 2002, U.S. President George W. Bush published the National Strategy to Combat Weapons of Mass Destruction, and stated that "interdiction is a critical part of the U.S. strategy to combat WMD and their delivery means. We must enhance the capabilities of our military, intelligence, technical, and law enforcement communities to prevent the movement of WMD materials, technology, and expertise to hostile states and terrorist organizations."[35]

President Bush reiterated the significance of this issue in a speech he delivered on 31 May 2003 in Krakow, Poland where he said "when weapons of mass destruction or their components are in transit, we must have the means and authority to seize them. So today I announce a new effort to fight proliferation called the Proliferation Security Initiative. The United States and a number of our close allies, including Poland, have begun working on new agreements to search planes and ships carrying suspect cargo and to seize illegal weapons or missile technologies. Over time, we will extend this partnership as broadly as possible to keep the world's most destructive weapons away from our shores and out of the hands of our common enemies."[36]

---

31 The formula meant, committing 10 billion USD from the United States and 10 billion USD from the other G-8 members combined, over a period of 10 years.

32 Participating states beyond the G-7 include Australia, Belgium, Czech Republic, Denmark, European Union, Finland, Hungary, Ireland, Kazakhstan, Mexico, Netherlands, New Zealand, Norway, Philippines, Poland, Republic of Korea, Sweden, Switzerland, and Ukraine.

33 Lynn Rusten et. al., "Building Security Through Cooperation", 2019, pp. 21-22.

34 National Institute Press, "The Proliferation Security Initiative: A Model for Future International Collaboration", 2009, p. 11, https://www.nipp.org/wp-content/uploads/2014/12/The-Proliferation-Security-Initiative-txt.pdf. (Accessed 15 December 2020)

35 The White House, "Statement by the President", *Office of the Press Secretary*, 11 December 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/12/20021211-8.html. (Accessed 15 December 2020)

36 Wawel Royal Castle, "Remarks by the President to the People of Poland", *Office of the Press Secretary,* The White House, 31 May 2003, http://georgewbushwhitehouse.archives.gov/news/release/2003/05/print/20030531-3.html. (Accessed 15 December 2020)

A significant number of states responded quickly to the call to participate in PSI. The first international meeting on implementing President Bush's PSI proposal took place in Madrid on 12 June 2003, less than 2 weeks after the Krakow speech. A factor that facilitated that speed and the subsequent rapidity of the actual establishment of PSI was the identity of the 11 participating governments in the initial PSI Core Group.[37] Most were longstanding allies of the United States in the North Atlantic Treaty Organization (NATO), in the G–8, or in the European Union (EU). Of the non-NATO members, Australia had long and close alliance ties with the United Kingdom and the United States, and Japan with the United States.[38]

From its inception, the Bush administration emphasized the informal nature of the PSI, characterizing it as an activity based on voluntary participation, rather than as an organization or institution. Besides, membership in the PSI does not entail any binding legal commitments. To join, states simply declare their commitment to the PSI Statement of Interdiction Principles either orally or in writing. The Statement of Interdiction Principles is a two-page document, essentially the "constitution" of PSI, outlining the purposes of the PSI and the general commitments of participant states, consisting of the interdiction of suspicious cargoes, the exchange of intelligence information related to proliferation, and the expansion of national legal authorities to support counter-proliferation. Conscious of the inherent difficulties in negotiating a multilateral treaty based on obtaining mutual compromise in specific issue areas, the framers of the PSI believed the activity could be established more efficiently and would receive the support of more states if it was based on voluntary participation rather than a binding legal agreement.[39]

Regular meetings among PSI participants devolved after March 2004 to the Operational Experts Group (OEG). After initial growth, the OEG has remained stable at 20 participants.[40] The members were chosen for their political significance, strong commitment to PSI, importance to international shipping, and/or regional distribution. Russia and Argentina joined the OEG largely because of political and regional factors respectively, and have been less active than other members. The OEG's fundamental role has been to translate the PSI principles into capabilities and action: planning and conducting exercises; identifying the capabilities and procedures required and available for interdictions, including legal basis; intelligence sharing; and sharing lessons learned from both successes and failures. In February 2004, President Bush. in a speech at the National Defense University (NDU), called for expansion of PSI to law enforcement to act directly against proliferators and that proposal was immediately and explicitly endorsed at the fifth PSI plenary meeting in March 2004.[41]

---

[37] Australia, France, Germany, Italy, Japan, Netherlands, Poland, Portugal, Spain, the United Kingdom and the United States.

[38] Susan J. Koch, *Proliferation Security Initiative: Origins and Evolution*, (Washington D.C.: National Defense University Press, June 2012), p. 10, https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Occasional%20Papers/09_Proliferation%20Security%20Initiative.pdf. (Accessed 15 December 2020)

[39] Philip Johnson, "Expanding the Proliferation Security Initiative: A Legal and Policy Analysis", *Defense Threat Reduction Agency*, Advanced Systems and Concepts Office, Report No. ASCO 2010 041, February 2010, p. 5.

[40] The participating states consist of the original 11 Core Group countries plus Argentina, Canada, Denmark, Greece, New Zealand, Norway, Russia, Singapore, and Turkey.

[41] Fort Lesley J. McNair, "President Announces New Measures to Counter the Threat of WMD: Remarks by the President on Weapons of Mass Destruction Proliferation", The White House, Office of the Press Secretary, 11 February 2004, https://georgewbush-whitehouse.archives.gov/news/releases/2004/02/20040211-4.html. (Accessed 15 December 2020)

PSI participants, especially through the OEG, emphasized a vigorous interdiction exercise program from the very beginning—with the first maritime exercise conducted just one week after the Statement of Interdiction Principles was issued in September 2003. Exercises have been essential in improving both national interdiction capabilities, and the ability of partners to work together under different scenarios. They also assist outreach to non-PSI members, many of whom have participated as observers. Since the inception of PSI, dozens of exercises were conducted, most of which have been dedicated live exercises, but there have been several command posts or table-top exercises as well. In the ensuing years, PSI scenarios have increasingly been included or "injected" into regular regional exercises.[42]

One of the most important measures of PSI's actual impact is its record of successful interdictions. The issue is surprisingly controversial, in large part because relatively little public information is available on the subject to protect sensitive information on intelligence and operational capabilities and procedures. The best-known PSI interdiction was both the first and the one with the most profound counter-proliferation impact. In early October 2003, just a few weeks after the issuance of the Statement of Interdiction Principles, the United States and the United Kingdom approached Germany and Italy regarding a shipment of nuclear centrifuge components destined for Libya. The supplier was A. Q. Khan,[43] whose network had manufactured the components at a clandestine factory in Malaysia and transshipped them through the United Arab Emirates. The carrier was the *BBC China*, a German-flagged vessel, giving the German government authority to board and search it (or to allow others to do so). Germany and Italy readily agreed to the interdiction, immediately citing their responsibilities under PSI. After the ship passed through the Suez Canal, the United States, United Kingdom, Germany and Italy worked together to divert it to a port in Italy.[44] The consequent exposure of Libya's nuclear weapons program and the unraveling of the A.Q. Khan network was a major factor contributing to Libya's decision two months later, in December 2003, to abandon its WMD and longer-range missile programs.[45]

Interdictions may be conducted against shipments of restricted goods, items that international treaties, export control regimes, or UN Security Council resolutions prohibit to be shipped internationally, or against dual-use items or materials which have both legitimate industrial or scientific applications as well as potential uses in WMD development programs, when such goods are shipped to states or non-state actors of proliferation concern.[46] Allowing PSI participants to determine which states should be subject to interdiction operations on the basis of subjective perceptions of proliferation activities is problematic precisely because the PSI has no independent legal authority and therefore the interdiction of shipments of

[42] National Institute Press, "The Proliferation Security Initiative: A Model for Future International Collaboration", 2009, p. 27.

[43] Abdel Qadeer Khan is a Pakistani nuclear physicist who is also known as the "father of Pakistani nuclear weapons program" because of his role in the uranium enrichment program of Pakistan.

[44] National Institute Press, "The Proliferation Security Initiative: A Model for Future International Collaboration", 2009, p. 28.

[45] Robert G. Joseph, *Countering WMD: The Libyan Experience*, (Fairfax: National Institute Press, 2009), pp. 40-41.

[46] U.S. Department of State, "PSI Interdiction Principles", Principle No. 1, 04 September 2003, https://www.state.gov/psi-interdiction-principles/. (Accessed 15 December 2020)

dual-use goods based on a determination by PSI participants that the end-user is an actor of proliferation concern amounts to an illicit interference in the free exchange of goods by non-origin or recipient states. Hence, critics portray PSI as a group of self-proclaimed world policemen violating international law and state sovereignty to enforce nonproliferation as they see fit. This is one of the greatest challenges not only to the operational capacity of the PSI, but also its perceived legitimacy and potential support by countries that are not currently participating in its activities.[47]

PSI has an impressive record of success. The Initiative has been effective in reinforcing international norms against proliferation, enhancing threat awareness, developing counter-proliferation capabilities, and improving habits and channels of cooperation among the member states, whose number has now reached 107. Yet there is still substantial room for improvement, including staying ahead of ever-changing proliferation practices while maintaining, and heightening, its original momentum. Moreover, the PSI approach of rapid, *ad hoc* international cooperative action, capacity building, and sharing information and lessons learned could also be usefully be applied to a multitude of international social and economic problems.[48]

United Nations Security Council Resolution 1540

This third good practice to be discussed has evolved within the framework of a United Nations Security Council (UNSC) resolution. In April 2004, recognizing the potentially grave consequences of a WMD terrorist attack anywhere in the World, the UNSC adopted Resolution 1540 under Chapter VII of the UN Charter and created binding obligations on all states to implement and enforce measures intended to combat the proliferation of nuclear, chemical, and biological weapons, as well as their means of delivery, to non-State actors. The Resolution requires that states implement domestic legislative and regulatory measures that prohibit non-state actors from developing or acquiring WMD and punish any non-state actors that seek to do so. The measures implemented must also apply to delivery systems and materials related to the design, development, production, use, transport, or transfer of such weapons. The Resolution stipulates various domestic controls that must be enacted related to physical security measures for weapons, delivery systems, and related materials; export and transshipment controls; border and law enforcement efforts to counter illicit trading of WMDs materials; prohibitions on proliferation financing, unauthorized transport, and any other services that would assist would-be non-state proliferators. The Resolution does not prescribe a precise formula or template that states must use to implement the controls listed above. As such, each state has some flexibility in implementing the measures in a manner appropriate to its legal system and national context.[49]

[47] Philip Johnson, *Expanding the Proliferation Security Initiative*, p. 9.

[48] National Institute Press, "The Proliferation Security Initiative: A Model for Future International Collaboration", 2009, pp. 46-49.

[49] Brian Finlay, "Meeting the Objectives of UN Security Council Resolution 1540: The Role of Civil Society", *Stimson Center*, December 2012, p. 4, http://www.vertic.org/media/assets/1540_Docs/Stimson%20meeting%20the%20objectives%20of%201540.pdf. (Accessed 15 December 2020)

Resolution 1540 has the potential to play an important role in forming universally recognized norms of state behavior with respect to WMDs. To do so, however, states must enact and enforce domestic controls over WMD material, wherever and whenever possible.[50] The Resolution calls for robust international cooperation in order to encourage broad compliance, on account of the implementation challenges likely to be faced by some member states. For many governments, significant barriers to compliance, including lack of implementation capacity, have prevented full implementation of the Resolution. As such, 1540 calls upon those member states and international organizations that are able, to provide appropriate assistance when requested, to states that lack the legal, financial, and/or other capacities to adequately implement the Resolution. Finally, the Resolution recognizes that cooperation with private industry, international and sub-regional organizations, and civil society is crucial for full and effective implementation of the mandate.[51]

A national export control system to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery is an essential instrument in meeting national obligations under Resolution 1540. It is for each state to decide on its national export control system in accordance with 1540. There is no single model for an export control system due to the great diversity in the legal and administrative systems of different countries. However, there are certain key elements which any export control system should have to be effective, including a clear legal basis establishing jurisdiction over relevant parties and activities; a transparent inter-agency coordination and decision-making mechanism for licensing or otherwise authorizing regulated behavior; enforcement authorities; and a capacity to actively reach out to industry to inform corporate actors of their obligations under national law.

In addition to exports, each state should also maintain appropriate national procedures or introduce and implement authority for the control over nuclear, chemical or biological weapons, and their means of delivery, including related materials and technologies within its jurisdiction, and including items in transit or being transshipped through its territory to a final destination outside its territory.[52] The *Best Practice Guide on UNSCR 1540 Export Controls and Transshipment* published by the Organization for the Security and Co-operation in Europe (OSCE) on 5 February 2010 provides information for developing or enhancing a national export control system over nuclear, chemical or biological weapons and their means of delivery, including related materials and technologies.[53]

---

[50] Jennifer M. Gibson and Sarah Shirazyan, "The UN Security Council Resolution 1540: An Overview of Extraterritorial Controls Over Non-State WMD Proliferation", *Nautilus Institute for Security and Sustainability*, NAPSNet Special Reports, 14 February 2012, https://nautilus.org/napsnet/napsnet-special-reports/the-un-security-council-resolution-1540-an-overview-of-extraterritorial-controls-over-non-state-wmd-proliferation/ (Accessed 15 December 2020)

[51] Finlay, "Meeting the Objectives of UN Security Council Resolution 1540: The Role of Civil Society", 2012, p. 5.

[52] *Ibid*.

[53] OSCE, "Best Practice Guide on UN Security Council Resolution (UNSCR) 1540 Export Controls and Transshipment", *FSC.DEL/65/09/Rev.3,* 16 September 2009, p. 1, https://www.osce.org/fsc/41446. (Accessed 15 December 2020)

To integrate the national processing of dual-use goods and conventional weapons through information sharing, the Conflict Prevention Center of the OSCE, in cooperation with United Nations Office for Disarmament Affairs (UNODA) and with the participation of the World Customs Organization (WCO), organized a workshop on customs procedures and licensing issuance in January 2012 in La Valetta, Malta. The general purpose of the workshop was to promote national inter-departmental and regional cooperation in export control licensing offices and customs services among OSCE Mediterranean Partners for Co-operation to contribute to countering the illicit trafficking of weapons and dual-use goods. The workshop also aimed to raise awareness of norms and measures that encourage information exchange among customs agencies at the regional level as well as to identify experiences and good practices as presented by the participating states that can facilitate implementation of the UNSCR 1540.[54]

Nuclear Security Summit Process

Fourth good practice discussed in this chapter arose out of the necessity to overcome one of the biggest hurdles in front of achieving the chief objective of securing the CBRN material worldwide, the lack of like-minded leadership in this regard among the top decision makers in the international political arena. Those who believe that terrorism with WMD is an exaggeration assert that scenarios involving terrorist use of WMD have been propagated purposefully by western intelligence agencies in order to incite fear among the less developed countries so as to manipulate their foreign and security policies.[55] To cite a specific example, as stated in an anecdote by Ambassador Román Oyarzun Marchesi, Chair of the 1540 Committee, "when it was adopted, the United Nations Security Council Resolution 1540 was seen by some as an unfortunate example of the North imposing new requirements on the South, indeed, dictating their domestic law."[56]

Prompted by similar complaints and criticisms voiced by a variety of sources, U.S. President Barack Obama launched the Nuclear Security Summit (NSS) in April 2010 to bring together heads of state and government from around the world in Washington DC in order to get their support for "an international effort to secure vulnerable nuclear materials within four years, break up black markets, detect and intercept materials in transit, and use financial tools to disrupt illicit trade in nuclear materials."[57]

---

[54] Regional Workshop on Customs Procedures and Licensing Issuance: Integrating the National Processing of Dual Use Goods and Conventional Weapons Through Information Sharing, 24-26 January 2012, La Valetta, Malta.

[55] Author's notes about the criticisms levelled by a wide range of high-ranking civil and military officers and academics against Prof. Graham T. Allison, Director, Belfer Center for Science and International Affairs, Harvard University, who made a presentation, titled "Nuclear Terrorism: The Ultimate Preventable Catastrophe" during the *Third International Symposium on Global Terrorism and International Cooperation* organized by the Centre of Excellence Defense Against Terrorism (COE-DAT) in Ankara, Turkey on 15 March 2010. https://www.tmmm.tsk.tr/publication/symposium_books/semp_book2010.pdf. (Accessed 15 December 2020)

[56] Román Oyarzun Marchesi, "Message from 1540 Chair", in Igor Khripunov (ed.), "1540 COMPASS", UNSCR, Winter 2016, No. 11, p. 3, http://spia.uga.edu/wp-content/uploads/2016/12/Compass_11-Winter2016.pdf. (Accessed 15 December 2020)

[57] The White House, "Addressing the Nuclear Threat: Fulfilling the Promise of Prague at the L'Aquila Summit", Office of the Press Secretary, 08 July 2009. https://web.archive.org/web/20120718040016/http://www.whitehouse.gov/the_press_office/Addressing-the-Nuclear-Threat-Fulfilling-the-Promise-of-Prague-at-the-LAquila-Summit/. (Accessed 15 December 2020)

In broader terms, the goal of the summit and the subsequent process that followed was to address the threat of nuclear terrorism by minimizing and securing weapons-usable civilian nuclear materials, enhancing international cooperation to prevent the illicit acquisition of nuclear material by terrorist groups and smugglers, and taking steps to strengthen the global nuclear security system. The NSS focus remained on nuclear material in the civil sphere and did not address the security of military nuclear material.[58] At the 2010 summit the participating countries have endorsed the consensus view that, given the security risks, the use of HEU outside military technologies should be minimized to the extent that it is technically and economically feasible. Several countries took individual steps to minimize or eliminate civil HEU.[59]

The summit meeting held in Washington DC in 2010 proved to be a novel idea and a very useful undertaking by the leaders, and thus they decided to carry on the process in the forthcoming years as well. Hence, subsequent meetings have taken place in Seoul, South Korea in 2012; the Hague, Netherlands in 2014; and again, in Washington DC in 2016. Each summit produced a consensus communiqué that reaffirmed the broad goals of the summit process and encouraged states to take actions, such as ratifying key treaties or minimizing stockpiles of weapons-usable materials. These voluntary and caveated recommendations were enhanced by individual, state-specific commitments made at each summit. These pledges, known as "house gifts," included actions such as repatriating weapons-usable materials, holding training for nuclear security personnel, updating national laws and regulations, and taking steps to combat illicit trafficking. At each subsequent summit, states reported on the progress made toward fulfilling these commitments.[60] At the 2012 summit in Seoul, groups of countries offered multinational commitments (gift baskets) that targeted key areas of nuclear security. In 2012, some 13 joint statements were offered. That number increased to 14 in the 2014 summit, with some gift baskets building on 2012 statements and others targeting new areas. At the latest summit in 2016, the participating states produced 21 gift baskets and agreed to five action plans for international organizations to take forward the conclusions of the summits.

While states, industry, and civil society committed to preserving the work undertaken at the summits, it was unclear how post-summit progress would be sustained under the presidency of Donald Trump when he took office in January 2017. Whereas the commitments emanating from the previous summits were being fulfilled by countries in a national capacity or through bilateral partnerships, there was no longer a central political mechanism to provide ongoing momentum to ensure that efforts would be coordinated during the Trump administration.[61]

---

[58] Kelsey Davenport, "Nuclear Security Summit at a Glance", *Arms Control Association*, June 2018, https://www.armscontrol.org/factsheets/NuclearSecuritySummit. (Accessed 15 December 2020)

[59] Miles A. Pomper, "Fighting Nuclear Terrorism: Phasing Out the Use of Highly Enriched Uranium in the Civil Sector", *Defence Against Terrorism Review*, Vol. 5, No. 1, Spring & Fall 2013, pp. 7-34.

[60] Kelsey Davenport, "Nuclear Security Summit at a Glance", 2018.

[61] Debra Decker, Lovely Umayam, Jacqueline Kempfer and Kathryn Rauhut, "Re-Energizing Nuclear Security: Trends and Potential Collaborations Post Security Summits", *Stimson Center*, Fall 2017, p. 16, https://www.stimson.org/wp-content/files/file-attachments/Nuclear-Energy-R7-WEB.pdf. (Accessed 15 December 2020)

Following the November 2020 presidential elections results, it remains to be seen at the time of the writing of this chapter if the presidency of Joe Biden will bring back the Summit process. But, there are reasons to be hopeful. First and foremost, Joe Biden used to be the former Vice-President during the Obama administration that launched and sustained the Nuclear Security Summit process. It is, therefore, highly likely that, in one form or another, the summit process may be on the agenda of Biden's administration. Second, countries that have participated in the NSS have, over the years, tried to institutionalize their nuclear security efforts through developing supportive follow-on action plans for the five international organizations, namely the United Nations, the IAEA, the INTERPOL, the Global Initiative to Combat Nuclear Terrorism (GICNT), and the G-8 Global Partnership. Finally, the role of civil society and non-governmental organizations (NGOs), which have participated in the summit process, is highly likely to endure.

Through fostering dialogue and conducting policy work, NGOs played a key role in supporting the mission of the Nuclear Security Summits. A coalition of about 80 international civil society groups seeking to reduce the threat of nuclear terrorism, including the author of this chapter, formed the Fissile Material Working Group (FMWG) to support the work of the summits and to coordinate NGO efforts in making recommendations to world leaders.[62] In addition to behind-the-scenes work with summit organizers to shape the agenda and the relevant deliverables, the FMWG held public conferences on the sidelines of each Nuclear Security Summit, convening hundreds of experts from the NGO community to discuss strategies to further improve our global nuclear security system. Furthermore, the FMWG's 2016 Nuclear Knowledge Summit agreed that future efforts to strengthen global nuclear security must be comprehensive, sustainable, focused on minimization, rigorous, and confidence-building. Going forward, the FMWG experts committed to track the progress toward greater nuclear security, provide education and training and cultivate collaboration among all stakeholders with a stake in nuclear security.[63]

Additional Measures to Keep Nuclear Material Safe and Secure

The Nuclear Security Guidelines (INFCIRC/225) of the International Atomic Energy Agency (IAEA), first issued in the 1970s, also are of fundamental importance in countering WMD terrorism. Although not mandatory, these guidelines have been adopted by most states and made a requirement through bilateral agreements. In the same vein, the IAEA's Illicit Trafficking Database Program (ITDP), involving the voluntary notification by government authorities of illicit trafficking incidents, provides a valuable source of information that helps the member states to better understand threats and vulnerabilities.

---

[62] The author has been a member of the FMWG and attended the Summits in Washington DC and in The Hague. The FMWG shifted to International Nuclear Security Forum (INSF) in October 2020. The INSF provides timely information to members, and focus on strengthening stakeholder knowledge and capacity by working with the nuclear security community to build stronger bridges between international experts. "International Nuclear Security Forum Launch", *Stimson*, https://www.stimson.org/event/the-international-nuclear-security-forum-launch/. (Accessed 15 December 2020)

[63] Debra Decker *et. al.*, *Re-Energizing Nuclear Security*, 2017, p. 18.

The Convention on the Physical Protection of Nuclear Material and Nuclear Facilities of 1987, with 161 states parties and 44 signatories as of June 2020, requires states to implement measures to prevent the theft, diversion or sabotage of nuclear material while being transported internationally. A 2005 Amendment extends the scope of the Convention to nuclear material in domestic use and storage, and to protection of nuclear facilities from sabotage.

The International Convention for the Suppression of Acts of Nuclear Terrorism, which was adopted in 2005 by the United Nations, with Russia and the United States being the first countries to sign, must be endorsed by more states in addition to the 115 states which have signed and ratified it.

The World Institute for Nuclear Security (WINS), was founded in Vienna in 2008 to contribute to achieving an equally important task: preventing the unauthorized transfer of nuclear expertise through the movement of trained personnel, including those in retirement. The risk of such personnel being recruited by terrorist groups is not negligible. In addition to the efforts of states and the international organizations, non-governmental organizations and the private sector must also be engaged, especially in addressing the inherent security risks associated with exporting advanced technologies, equipment, and material. WINS is an institution that aims to share information and experience among the industry nuclear security professionals, as well as promoting training.

Turkey's Policy and Practice to Counter WMD Terrorism

Without doubt, as a NATO member and a state party to all of the WMD nonproliferation treaties and conventions, strengthening these regimes is in Turkey's primary interest. Therefore, Turkey assigned priority to assisting international efforts to counter the threat of WMD terrorism and adopted the good practices mentioned in the previous sections in devising and implementing its export control regime so as to effectively meet the challenge of countering WMD terrorism.

Accordingly, Turkey declared its support to the Proliferation Security Initiative as soon as it was launched by the United States in May 2003. Turkey, while following other PSI activities, has itself hosted land, sea and air interdiction PSI exercises, first in May 2006 and in successive years with the participation of dozens of guest nations, and continues to actively contribute to the PSI. Pursuing an active policy against terrorism, Turkey joined, as initial partner state, the Global Initiative to Combat Nuclear Terrorism. Ankara hosted the GICNT's second meeting in 2007. Turkey has also welcomed UN Security Council Resolution 1540, and, with a view to fulfilling the provisions of international non-proliferation instruments and arrangements to which Turkey is party, an enhanced system of export controls is implemented. Turkey submitted its first report in November 2004 and has regularly updated its reports over the years. Last update was made in August 2020 but this living document requires constant updates as changes take place in legislation and international commitments. Due to delays

caused by the coronavirus pandemic, all activities related to Comprehensive Review on the status of implementation of resolution 1540, including the open consultations, are currently postponed to 2021.[64]

Turkey has also taken a number of steps to counter illicit trafficking, such as acceding to participation in the Nuclear Suppliers Group (NSG) in 1999.[65] Accordingly, Turkey has undertaken the process of adjusting its national export control regime (i.e., laws and regulations) to that of the NSG countries. Currently, the Turkish export control system is in line with the European Union's standards. Turkish national legislation, developed in the context of the country's safeguards agreement and other IAEA protocols, provides Turkish authorities with the legal basis to control the materials and equipment covered by the list of the NSG. Concomitantly with its application to the NSG, Turkey has undertaken the same stance toward the Zangger Committee and became a member soon after its Foundation in 1999. This has been considered by Turkish security authorities as an almost automatic outcome of the formal accession to the NSG. Turkey also joined the Australia Group in 1999. Since then, it has taken steps to include all the items of the various export lists, which often differ by one or two items from the other universal export control lists. Turkey also became a member of the Missile Technology Control Regime (MTCR) in April 1997. Since then, Turkish delegations have been active in participating in the meetings of member states as well as promoting new ideas with a view to rendering the controls much more effective.

Turkish law enforcement authorities cooperate with international agencies such as INTERPOL to promote national and regional interagency collaboration to counter nuclear smuggling. Turkey is also a participant of the U.S. State Department's Export Control and Related Border Security Program (EXBS) which provides radiation interdiction training and equipment to Turkish law enforcement agencies. Turkish authorities maintain that the success of the export control regimes will depend on the continuous and coordinated exercise of vigilance and restraint in transfers, especially to the regions of concern. Similarly, the collective capability of the regime to foresee developments and to be proactive in devising measures to reverse threatening proliferation trends is also crucial for the successful implementation of export control regimes.[66]

Inspired by the cases discussed above, Turkey devised and implemented an export control system which is based on continuous inter-agency coordination and consultation, which involves the Ministry of Trade, the Ministry of Forestry and Agriculture, the Ministry of

---

[64] Notes from the presentation of Berna Kasnaklı Versteden, Minister-Plenipotentiary, Deputy Director General for OSCE, Arms Control and Disarmament, Turkish Ministry of Foreign Affairs, titled "Turkey's Counter-Proliferation Policy & Efforts" during the *Counter Proliferation of WMD in MSO Course*, organized by the Multinational Maritime Security Centre of Excellence (MARSEC COE) in Istanbul, Turkey on 20-22 October 2020.

[65] Mustafa Kibaroglu, "Nuclear Security and Turkey: Dealing with Nuclear Smuggling", in Sinan Ulgen (ed.), *Nuclear Security: A Turkish Perspective*, (Istanbul: EDAM and Nuclear Threat Initiative, 2015), pp. 77-94. https://edam.org.tr/wp-content/uploads/2015/01/edam_nucphysec2015_full.pdf. (Accessed 15 December 2020)

[66] Mustafa Kibaroglu and Nilsu Goren, "Emerging Safety, Security and Peaceful Nature of Nuclear Energy in Turkey", Unpublished Manuscript, 2014.

Foreign Affairs, the Ministry of National Defense, the Nuclear Regulatory Authority and the Exporters' Unions. Through the interaction of these agencies within a mutually reinforcing, multi-layered system of licensing, registration and control, Turkey can effectively track the movement of listed items in and out of the country.[67]

The export of sensitive and dual-use materials covered by international instruments and export regimes is controlled by virtue of a two-tier mechanism that involves separate processes of licensing by the Ministry of National Defense for military equipment, arms and ammunition and the Nuclear Regulatory Authority for dual-use items described in the NSG control list, along with registration by the Ministry of Economy. For military equipment, arms and ammunition, the first tier is regulated by Law Number 5201 dated 03 July 2004, which replaced original Law Number 3763 of 1940 regarding "The Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment and Ammunition." This law requires licenses to be obtained from the Ministry of National Defense for the export of all weapons and ammunition. The Ministry of National Defense issues every year a list of all weapons, ammunition, explosive materials and their parts, which are subject to licensing. Items listed in the NSG list, are regulated by the "Regulation on Export Licensing of Materials, Equipment and Related Technologies Employed in the Nuclear Field" published in the *Official Gazette* on 15 February 2000, No: 23965, and updated in 2007 (*Official Gazette* No. 26642 on 19 September 2007).[68]

As to the second tier, it is the duty of the Ministry of Treasury and Finance to take all monitoring, control, arrangement and orientation measures regarding exports and to draft the general export policy of Turkey. In fulfilling its duties, the Ministry of Treasury and Finance avails itself of the 13 exporters' unions located around the country. Istanbul Metals and Minerals Exporters' Union (IMMIB), like other exporters' unions, is responsible for the implementation of the general export policy, under the auspices of the Ministry of Treasury and Finance. All exporters are required to be a member of an exporters' union in order to be able to export any good or material. Sensitive goods, technologies and dual-use materials are registered by IMMIB, which denotes this registration on the customs declaration. This mechanism enables centralized monitoring of the export of sensitive goods, technologies and dual-use materials on the basis of exporting company, product, quantity and value. IMMIB determines whether or not the goods to be exported are subject to export controls. If so, then this export is submitted to the procedure described above, where permissions from relevant institutions are sought.

Conclusion

The issues that are discussed in the above sections suggest that contingencies involving the use of WMD by terrorist groups must be considered within the context of "low probability

[67] Notes from the presentation of Berna Kasnaklı Versteden.
[68] Kibaroglu and Goren, "Emerging Safety, Security and Peaceful Nature of Nuclear Energy in Turkey", 2014.

vs high consequence" scenarios. The absence of such horrific incidents to date has not been because of the reluctance of terrorist organizations in resorting to CBRN material in their attacks, but it was thanks to the concerted efforts of the responsible authorities in concerned governments around the world and in international organizations who have done their best to devise and implement the effective practices discussed in this chapter, and much more, for effectively safeguarding the sensitive material, technology and know-how that are widely available in many countries to keep them away from the reach of the terrorists.

Bearing in mind the fact that the intolerable consequences of WMD terrorism would transcend the political boundaries of the countries where such attacks may occur, the good practices that are mentioned above must be pursued relentlessly by every single government in the world, regardless of the conjunctural developments in the international arena and the divergent national interest calculus of each state that may, at times, make cooperation and collaboration difficult. One particular rule must always be remembered in the fight against terrorism, which is that terrorists need to be successful only once in their attempts, while governments must be successful at all times in countering them.

Bibliography

Ackerman, Gary and Jacome, Michelle, (2018), "WMD Terrorism: The Once and Future Threat", *PRISM*, Vol. 7, No. 3, 18 May 2018, pp. 23-36, https://cco.ndu.edu/Portals/96/Documents/prism/prism7_3/180515_Ackerman_PCP.pdf?ver=2018-05-18-174850-983. (Accessed 15 December 2020)

Allison, Graham T., (2004), *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, (New York: Times Books, Henry Hold & Company).

Allison, Graham T., (2010), "Nuclear Terrorism: The Ultimate Preventable Catastrophe" presented at Third International Symposium on Global Terrorism and International Cooperation, Centre of Excellence Defense Against Terrorism (COE-DAT), 15 March 2010, https://www.tmmm.tsk.tr/publication/symposium_books/semp_book2010.pdf. (Accessed 15 December 2020)

Aytac, Osman, and Kibaroglu, Mustafa (eds.), (2009), *Defense Against Weapons of Mass Destruction Terrorism*, (Amsterdam: IOS Press).

Blum, Andrew, Asal, Victor, Wilkenfeld, Jonathan, Steinbruner, John, Ackerman, Gary, Gurr, Ted Robert, Stohl, Michael, Post, Jerrold M., Sinai, Joshua, LaFree, Gary, Dugan, Laura, Franke, Derrick, Stanislawski, Bartosz H., Sheffer, Gabriel, Lichbach, Mark Irving, Sandler, Todd, and Enders, Walter, "Nonstate Actors, Terrorism, and Weapons of Mass Destruction", *International Studies Review*, Vol. 7, No. 1, March 2005, pp. 133-170.

Bunn, Matthew, Tobey, William H., Malin, Martin B., and Roth, Nickolas, (2016), "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?", *Belfer Center for Science and International Affairs*, Project on Managing the Atom, March 2016, https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf. (Accessed 15 December 2020)

Cankaya, Selcuk, and Kibaroglu, Mustafa (eds.), (2010), *Bioterrorism: Threats and Deterrents,* (Amsterdam: IOS Press).

Castle, Wawel Royal, (2003), "Remarks by the President to the People of Poland", *Office of the Press Secretary,* The White House, 31 May 2003, http://georgewbushwhitehouse.archives.gov/news/release/2003/05/print/20030531-3.html. (Accessed 15 December 2020)

Congressional Research Service, "The Evolution of Cooperative Threat Reduction: Issues for Congress", CRS Report R43143, 23 November 2015, https://fas.org/sgp/crs/nuke/R43143.pdf. (Accessed 15 December 2020)

Davenport, Kelsey, (2018), "Nuclear Security Summit at a Glance", *Arms Control Association*, June 2018, https://www.armscontrol.org/factsheets/NuclearSecuritySummit. (Accessed 15 December 2020)

Decker, Debra, Umayam, Lovely, Kempfer, Jacqueline, and Rauhut, Kathryn, (2017), "Re-Energizing Nuclear Security: Trends and Potential Collaborations Post Security Summits", *Stimson Center*, Fall 2017, https://www.stimson.org/wp-content/files/file-attachments/Nuclear-Energy-R7-WEB.pdf. (Accessed 15 December 2020)

Defense Threat Reduction Agency, (2013), "Nunn-Lugar CTR Scorecard," May 2013, https://www.dtra.mil/Portals/61/Documents/20130501_fy13_ctr-scorecard_slides_may13.pdf (Accessed 15 December 2020)

Ferguson, Charles Daniel and Smith, Michelle M., (2009), "Assessing Radiological Weapons: Attack Methods and Estimated Effects," *Defence Against Terrorism Review*, Vol. 2, No. 2, Fall 2009, pp. 15-34.

Finlay, Brian, (2012), "Meeting the Objectives of UN Security Council Resolution 1540: The Role of Civil Society", *Stimson Center*, December 2012, p. 4, http://www.vertic.org/media/assets/1540_Docs/Stimson%20meeting%20the%20objectives%20of%201540.pdf. (Accessed 15 December 2020)

Forest, James, (2012), "Framework for Analyzing the Future Threat of WMD Terrorism," *Journal of Strategic Security,* Vol. 5, No. 4, pp. 51-68.

Franz, David R., (1998), "The Role of Biotechnology in Countering BTW Agents," paper presented at NATO Advanced Research Workshop, 21-23 October 1998.

Gibson, Jennifer M., and Shirazyan, Sarah, (2012), "The UN Security Council Resolution 1540: An Overview of Extraterritorial Controls Over Non-State WMD Proliferation", *Nautilus Institute for Security and Sustainability*, NAPSNet Special Reports, 14 February 2012, https://nautilus.org/napsnet/napsnet-special-reports/the-un-security-council-resolution-1540-an-overview-of-extraterritorial-controls-over-non-state-wmd-proliferation/ (Accessed 15 December 2020)

Harahan, Joseph P., (2014), *With Courage and Persistence: Eliminating and Securing Weapons of Mass Destruction with the Nunn-Lugar Cooperative Threat Reduction Programs*, (Washington D.C.: Defense Threat Reduction Agency), https://www.dtra.mil/Portals/61/Documents/History/With%20Courage%20and%20Persistence%20CTR.pdf?ver=2016-05-09-102902-893. (Accessed 15 December 2020)

Hoffman, Bruce, (2007), "CBRN Terrorism Post 9/11", in Russell D. Howard and James Forest (eds.), *Weapons of Mass Destruction Terrorism*, (New York: McGraw Hill).

IAEA, "Research Reactor Database, https://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx?filter=0. (Accessed 15 December 2020)

IAEA, "The Database on Nuclear Power Reactors", https://pris.iaea.org/PRIS/home.aspx. (Accessed 15 December 2020)

Igor Khripunov (ed.), (2016), "1540 COMPASS", UNSCR, Winter 2016, No. 11, http://spia.uga.edu/wp-content/uploads/2016/12/Compass_11-Winter2016.pdf. (Accessed 15 December 2020)

Johnson, Philip, (2010), "Expanding the Proliferation Security Initiative: A Legal and Policy Analysis", *Defense Threat Reduction Agency*, Advanced Systems and Concepts Office, Report Number ASCO 2010 041, February 2010.

Kazi, Reshmi, (2011), "The Correlation Between Non-State Actors and Weapons of Mass Destruction, *Connections*, Vol. 10, No. 4, pp. 1-10.

Kibaroglu, Mustafa, (2014), "The Threat of Nuclear Terrorism Requires Concerted Action" *Strategic Analysis*, Vol. 38, No. 2, March 2014, pp. 209-216.

Kibaroglu, Mustafa, and Goren, Nilsu, "Emerging Safety, Security and Peaceful Nature of Nuclear Energy in Turkey", Unpublished Manuscript, 2014.

Koch, Susan J., (2012), *Proliferation Security Initiative: Origins and Evolution*, (Washington D.C.: National Defense University Press), https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Occasional%20Papers/09_Proliferation%20Security%20Initiative.pdf. (Accessed 15 December 2020)

Mark, Carson, Taylor, Theodore, Eyster, Eugene, Maraman, William, and Wechsler, Jacob, (2002), "Can Terrorists Build Nuclear Weapons*?" Nuclear Control Institute,* https://www.nci.org/k-m/makeab.htm. (Accessed 15 December 2020)

McNair, Fort Lesley J., (2004), "President Announces New Measures to Counter the Threat of WMD: Remarks by the President on Weapons of Mass Destruction Proliferation", Office of the Press Secretary, The White House, 11 February 2004, https://georgewbush-whitehouse.archives.gov/news/releases/2004/02/20040211-4.html. (Accessed 15 December 2020)

Medalia, Jonathan E., (2011) "'Dirty Bombs': Technical Background, Attack Prevention and Response, Issues for Congress"*, Congressional Research Service,* R41891, 24 June 2011, https://fas.org/sgp/crs/nuke/R41890.pdf, (Accessed 15 December 2020)

Mowatt-Larssen, Rolf. (2010), "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" *Belfer Center for Science and International Affairs,* January 2010, https://www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality. (Accessed 15 December 2020)

National Institute Press, (2009), "The Proliferation Security Initiative: A Model for Future International Collaboration", https://www.nipp.org/wp-content/uploads/2014/12/The-Proliferation-Security-Initiative-txt.pdf. (Accessed 15 December 2020)

National Institute Press, (2009), "The Proliferation Security Initiative: A Model for Future International Collaboration".

Nikitin, Mary Beth, and Woolf, Amy F., (2015) "The Evolution of Cooperative Threat Reduction: Issues for Congress", *Congressional Research Service*, CRS Report No. R43143, November 2015, https://fas.org/sgp/crs/nuke/R43143.pdf. (Accessed 15 December 2020)

NTI, (2015), "The Biological Threat", https://www.nti.org/learn/biological/. (Accessed 15 December 2020)

OPCW, "OPCW by the Numbers", https://www.opcw.org/media-centre/opcw-numbers. (Accessed 15 December 2020)

OSCE, (2009), "Best Practice Guide on UN Security Council Resolution (UNSCR) 1540 Export Controls and Transshipment", *FSC.DEL/65/09/Rev.3,* 16 September 2009, https://www.osce.org/fsc/41446. (Accessed 15 December 2020)

Pomper, Miles A., (2013), "Fighting Nuclear Terrorism: Phasing Out the Use of Highly Enriched Uranium in the Civil Sector", *Defence Against Terrorism Review*, Vol. 5, No. 1, Spring & Fall 2013, pp. 7-34.

Robert G. Joseph, (2009), *Countering WMD: The Libyan Experience*, (Fairfax: National Institute Press).

Roberts, Brad (ed.), (2000), *Hype or Reality? The "New Terrorism" and Mass Casualty Attacks*, (Alexandria: The Chemical and Biological Arms Control Institute).

Rusten, Lynn, Johnson, Richard, Andreasen, Steve, and Severance, Hayley Anne, "Building Security Through Cooperation", *Nuclear Threat Initiative*, 2019, https://media.nti.org/pdfs/NTI_DPRK2019_RPT_FNL.pdf. (Accessed 15 December 2020)

Salama, Sammy and Hansell, Lydia, (2005), "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *The Nonproliferation Review,* Vol. 12, No. 3, pp. 615-653.

Shields, John M., and Potter, William C. (eds.), (1997), *Dismantling the Cold War: U.S. and NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program*, (Cambridge: The MIT Press).

Sinan Ulgen (ed.), (2015), *Nuclear Security: A Turkish Perspective*, (Istanbul: EDAM and Nuclear Threat Initiative), https://edam.org.tr/wp-content/uploads/2015/01/edam_nucphysec2015_full.pdf. (Accessed 15 December 2020)

Stenersen, Anne, (2008), *Al-Qaida's Quest for Weapons of Mass Destruction: The History behind the Hype*, (Riga: VDM Verlag Dr. Müller).

Stimson, "International Nuclear Security Forum Launch", https://www.stimson.org/event/the-international-nuclear-security-forum-launch/. (Accessed 15 December 2020)

The White House Office of the Press Secretary, (2002), "Statement by the President", 11 December 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/12/20021211-8.html. (Accessed 15 December 2020)

The White House, (2009), "Addressing the Nuclear Threat: Fulfilling the Promise of Prague at the L'Aquila Summit", Office of the Press Secretary, 08 July 2009. https://web.archive.org/web/20120718040016/http://www.whitehouse.gov/the_press_office/Addressing-the-Nuclear-Threat-Fulfilling-the-Promise-of-Prague-at-the-LAquila-Summit/. (Accessed 15 December 2020)

Tucker, Jonathan B. (ed.), (2000), *Toxic Terror, Assessing Terrorist Use of Chemical and Biological Weapons*, (Cambridge: MIT Press).

U.S. Department of State, "PSI Interdiction Principles", Principle No. 1, 04 September 2003, https://www.state.gov/psi-interdiction-principles/. (Accessed 15 December 2020)

United Nations General Assembly, (2004), A More Secured World: Our Shared Responsibility: Report of the High-level Panel on Threats, Challenges and Change, A/59/565, 02 December 2004, p. 21. https://www.un.org/ruleoflaw/files/gaA.59.565_En.pdf. (Accessed 15 December 2020)

Versteden, Berna Kasnaklı, (2020), "Turkey's Counter-Proliferation Policy & Efforts" presented at Counter Proliferation of WMD in MSO Course, Multinational Maritime Security Centre of Excellence (MARSEC COE), 20-22 October 2020.

Voica, Dan Radu, and Kibaroglu, Mustafa (eds.), (2011), *Responses to Nuclear and Radiological Terrorism*, (Amsterdam: IOS Press).

Walker, Paul, (2006), "Nunn-Lugar at 15: No Time to Relax Global Threat Reduction Efforts", *Arms Control Today*, May 2006, https://www.armscontrol.org/act/2006-05/features/nunn-lugar-15-time-relax-global-threat-reduction-efforts. (Accessed 15 December 2020)

Zimmerman, Peter, (2009), "Do We Really Need to Worry? Some Reflections on the Threat of Nuclear Terrorism", *Defence Against Terrorism Review,* Vol. 2, No. 2, Fall 2009, pp. 1-14.

CHAPTER VII

MEDIA AND COUNTER-TERRORISM

Afzal Ashraf
Stephanie Foggett

Introduction

The North Atlantic Treaty Organization's (NATO) direct counter-terrorism (CT) responsibilities are limited, being largely eclipsed by member states' and host nation responsibility and the primacy of civil over military responsibility in this field. What NATO actually does in terms of direct CT is, however, crucial and almost everything the Alliance does operationally is in an environment where terrorism exists, to varying degrees. In many cases, NATO also provides training and governance capacity building activities to allied and partner countries and international organisations responsible for CT. For all of these reasons, an understanding of how terrorist actors use the media and communications landscape, including emerging media platforms, and of how CT organisations can respond to this challenge is of considerable importance to the Alliance.

This chapter lays out why it is critically important for NATO, host nations, and partners to understand the contemporary media and communications landscape and how it intersects with security challenges, with a primary focus on international terrorism. First, this chapter begins by looking at the utility and importance of media and communications to terrorist actors and in so doing makes a distinction between the message and the medium.

Second, the chapter will focus on online communications but will also look at 'mass communication'[1] more generally, to evaluate how terrorists take advantage of contemporary channels, including television, radio, press and other mass media, as well as newer online spaces and social media. The relationship between conventional mass communications and online, especially social media, will be explored to determine the increasingly interdependent nature of these two mediums. How the contemporary media and communications space is being utilized by terrorist actors and extremist groups for a range of other activities will also be explored. Analysis throughout this chapter assumes the simultaneous and multiple use of communication mediums for activities such as propaganda, intelligence gathering, surveillance, recruitment, fundraising etc.

[1] See Paul Wilkinson's definition of mass media: "The mass media are taken to encompass newspapers, radio and television, but other important forms of communications include books, films, music etc." Wilkinson, *The media and terrorism*, 51-64.

Third, there is – understandably – a significant focus on leveraging media and communications strategies, tools and programmes in support of CT, especially in counter-messaging and counter-narrative work. This chapter cautions, however, that there is presently limited evidence that terrorist violence can be countered in this way or that it is preferable to other programmes that might provide support to individuals vulnerable to radicalisation and recruitment, such as psychosocial support programmes.[2] Further, the chapter cautions whether a military entity, like NATO, should be a lead actor on such work. This section will provide some observations and suggestions for NATO to improve its awareness and understanding of the evolving and expanding challenge of terrorists' use of the internet, in particular their exploitation of social media platforms. These will be considered in both a passive and offensive as well as in a policy and operational context.

Finally, the chapter will conclude with some military-specific considerations for the Alliance. While the terrorism and media discussion has relevant historical, political and policy considerations for NATO; it is also important for militaries to defend their reputation during operations, including CT operations, by making it clear, through media and communications, what the military is responsible for and what the political power is responsible for. A blurring between these lines of responsibility can present challenges for a military in the future and can weaken fundamental communications functions like providing trusted public information and delivering effective emergency and crisis response communications.

Terrorism & Media's 'Symbiotic Relationship'

The utility and importance of media and communications to terrorist actors has been widely recognised by scholars and observers of terrorism for decades. Further, a historical approach reveals that international terrorism and attempts to counter it both militarily and politically go back over a century. There is a propensity for analysts to be mesmerised by the medium at the expense of the message.[3] The majority of CT analysis in the military context is rightly focussed on identifying *who* poses a threat and *what* that threat is so that it can be effectively countered. In the media or communication context that analysis should aim to understand *why* the threat exists and *how* it should be stopped. All terrorism is designed to convey a message and knowing what that message is provides a basis for countering not just the message but the underlying rationale of terrorist actors.

Subsequently, both the historical and contemporary discourse on media and terrorism is borne out of the understanding that some form of synergy exists between the two. More simply put "terrorism and the media are bound together in an inherently symbiotic relationship," notes terrorism scholar Bruce Hoffman.[4] The fundamentals of this synergy are best explained by Paul Wilkinson[5]: "For terrorism by its very nature is a psychological weapon which depends upon communicating a threat to the wider society. This, in essence, is why terrorism and

2 Moonshot, *Social Grievances*.
3 Ashraf, *Terrorism and Propaganda*.
4 Hoffman, *Inside Terrorism*.
5 Wilkinson, *The media and terrorism*.

the media enjoy a symbiotic relationship." For governments and international organisations, like NATO, it becomes critically important to understand the dynamics and evolution of this relationship. Traditionally, this discourse has looked at the impact of press and media coverage (television, radio, print etc.); today, however, terrorism study must also factor in social media and the use of new and evolving digital communications and technology platforms and their influence and impact on terrorism and CT.

Indeed, the distinction between traditional media[6] and new media adds an additional layer of complexity to the discourse on media and terrorism, which will be further explored later in the chapter. Traditional media facilitated one-way communication able to deliver a carefully crafted message to an audience; new media and social media, on the other hand, is designed as two-way communication, intended to deliver a message and to initiate a conversation or interaction with the audience. Further, traditional media is less immediate, with trained editors or producers determining what their audiences would see before publication or broadcast; new media is designed to be instant with terrorist groups and extremist actors now able to determine in real-time what their audiences will see, when they will see it, and how they will see it.[7] The 'symbiotic relationship' between media and terrorism and the contemporary media and communications landscape, in particular the rise and evolution of new media and social media, shifts the calculus on how best to understand and manage the complex and evolving synergy that exists between the two.

Lastly, much of the historical and contemporary terrorism discourse tends to problematise the role of media and communications. Cristina Archetti, for example, challenges the idea that new recruits to terrorism are 'radicalized' by a 'narrative of grievance'; that the removal of extremist websites should be a priority; that 'we' can 'rewrite' terrorists' propaganda; that being a 'global brand' is a source of strength.[8] She, nevertheless, agrees that terrorist groups should be challenged through the internet, albeit through a different approach. Security and political actors like NATO, and the host and partner countries which interact with the Alliance, should therefore not lose sight of the greater importance of media and communications, in particular traditional media, to a democratic society. CT efforts should not stifle the media or operate at the expense of freedom of speech and freedom of expression; this can in turn undermine democratic society and the credibility of the media in the first place.[9] For such reasons, an understanding of terrorism and the media would be remiss without recognizing the greater importance of the media to a democratic society and the freedoms and values it fights for in the first place. *Washington Post* publisher Katherine Graham poignantly made this case in 1986: "Terrorists, in effect, hang themselves whenever they act. They convey hatred, violence, terror itself...Publicity may be the oxygen of terrorists. But I say this: News is the lifeblood of liberty. If the terrorists succeed in depriving us of freedom, their victory will be far greater than they ever hoped and far worse than we ever feared".[10]

---

6 Traditional media can be defined as any form of mass communication used before the advent of digital media including TV, radio, newspapers and journals.

7 Jenkins, *The New Age of Terrorism*.

8 Archetti, *Understanding Terrorism.*

9 Marthoz, *Terrorism and the Media*.

10 Graham, *Safeguarding Our Freedoms*.

If news is the lifeblood of liberty, then fake news risks fatally haemorrhaging democracies. Fake news is used to "manage public opinion, control the social situation, form a specified impression or justify someone's policy and action".[11] All of these objectives align with the needs of democratic politics. The invisible line between political persuasion and manipulation, which has never existed in totalitarian states, has now been dangerously eroded in democracies to the extent that even senior political leaders in NATO have discredited mass media as 'fake news' rather than defend it as an institution crucial to the security of the democratic system. The consequence is a "predictable and significant decline in confidence in the traditional media. Society is gradually becoming more selective about information, which raises the popularity and demand for independent media sources"[12] These 'independent' sources are often anything but independent. They tend to carry a subjective agenda, in opposition to NATO's aims. They can be echo chambers for increasingly polarised and extreme opinion. Further, extremist actors have entered the mis- and dis-information fray, as was witnessed when a white nationalist group incited violence using a fake account on Twitter during protests in the United States in 2019.[13] If the media is to be NATO's weapon in the war against terrorism, then its most senior political leaders are unwittingly scuttling it. Before any good practice is considered, NATO will need to explain to the political leadership of its member states the importance of credible, professional and reliable journalism underpinning a critical, balanced and objective mass media. Without it, however compelling NATO's CT message, it will be largely mute and ignored.

The Evolving Media and Communications Landscape

Amongst the dramatic changes in the contemporary media landscape are a complex fusion and interplay between traditional media and mass media[14] and social media and communication applications on the Internet. Boundaries between them have become blurred and it is almost impossible to devise distinct or separate strategies for mass media and social media. Overall, there has been a demonstrable shift from one-way communication to a two-way dialogue. There has been a change from slightly delayed editorially mediated content to unfiltered and immediate access to information. Most significantly, there has been self-imposed segregation in both mass media and social media with groups of people gravitating towards sources of information that reinforce, rather than challenge their worldviews, beliefs and prejudices. This situation creates echo chambers ripe for extremist narratives to exploit and serves to isolate and inoculate groups from counter messages.

---

[11] Berduygina, Vladimirova and Chernyaeva, *Trends in the Spread*, 122-132.

[12] *Ibid.*

[13] Collins, Zadrozny and Saliba, *White nationalist group.*

[14] The terms mass media and traditional are often used interchangeably. The difference between them is that mass media provides some indication of the reach and impact of various forms of traditional media. For example, TV, radio and press can be local in their reach. However, if they are able to broadcast at a national or international level then they might be more accurately defined as mass media. Similarly, the term new media encompasses communication systems such as social media, direct communication apps such as WhatsApp and telegram and websites. It can also include email and telephone applications such as text. Traditional and Mass media is growingly using new media as a platform or as a means of signposting to increase its reach.

These changes have represented both a challenge and an opportunity. The ongoing 'digital revolution' means that most of the world's population now have widescale access to mobile devices, tablets, computers and the Internet.[15] Information actors – whether from media, entertainment or sport; products, brands and businesses; or state actors, governments, and international organisations, among many others – all now have a higher digital penetration rate for accessing audiences, consumers, communities, and citizens worldwide. Since terrorist and extremist groups are also information actors, they too now have a wider reach and larger audience potential because of media and technological advancements. Evidence indicates that terrorist and extremist actors have been able to adapt and exploit these opportunities, utilising communication mediums and the online space for a range of activities, to include propaganda, radicalisation, recruitment, fundraising, operations and other actions.[16]

State actors, governments, and international organisations, like NATO, are correct to recognize the wider array of opportunities now available to them to enhance communications, produce new media, and engage wider and more diverse audiences. However, successfully navigating the evolving media landscape from a CT perspective has proven to be a complex and complicated endeavour. For example, despite considerable resources and much effort by way of campaigns and initiatives, states and militaries have yet to demonstrate sustainable successes in the exploitation of this environment. Many media strategies devised to support CT, most notably in counter-narrative and counter-messaging initiatives, are based on unproven hypotheses. There is also a problem with the measurement of effect with such activities, meaning that there is little reliable data to suggest that success has been or could be delivered. The discussion is further bounded by the impact of wider issues such as legal, social and privacy constraints.

Communications-Based Responses to Terrorism

In light of the vast developments in the contemporary media and communications landscape, understanding the relationship between media and terrorism today remains paramount. Perhaps the most fundamental questions on this topic are whether and how violent words, images or narratives lead to violent actions. To answer such questions would require a consistent framework for measurement, which is notoriously lacking in preventing or countering violent extremism (P/CVE). A 2018 study by the RAND Corporation identified three key challenges of measuring CVE: 1) multiple pathways to violent extremism; 2) difficulties detecting and measuring violent extremism attributes, like internalised emotions; 3) and that evaluation of CVE is political and ambiguous.[17] A study the same year by the United States Institute of Peace (USIP) similarly noted "there is no defined set of practices, methods, or approaches used to evaluate the impact of programs that have the goal of preventing or countering violent extremism (P/CVE), reflecting the nascent and diverse nature of the field".[18] Perhaps the greatest difficulty in measures of effects involving prevention is that it is almost impossible to directly measure something that has been successfully prevented from happening.

[15] Kemp, *Digital 2020*.
[16] United Nations Office of Drugs and Crime (UNODC), *The Use of the Internet*.
[17] Baruch, Ling, Warnes, and Hofman, *Evaluation in an emerging field*, 475-495.
[18] Holmer, Bauman, and Aryaeinejad, *Measuring Up*.

Further, the role of media, communications and narratives factors heavily in contemporary CVE discourse. Yet, similarly to the challenge faced by CVE as a whole, the sub focus on 'counter-messaging' or 'counter-narratives' is equally underdeveloped. "Counter-narrative approaches to violent extremism are currently built on weak foundations, theoretically and empirically," notes Andrew Glazzard.[19] A review by Kate Ferguson of CVE through media and communications strategies concluded there was little hard evidence on the interaction between violent content and participation in violent activities. Further, her study also noted a lack of evidence that violent extremism can be countered by an alternative set of communications.[20]

A recent analytical brief by the United Nations CT Committee Executive Directorate (CTED) noted the numerous challenges on deciding whether and how to engage in countering terrorist narratives online, including criticism of the lack of monitoring and evaluation of counter-narrative initiatives.[21] The notion of countering terrorist propaganda with credible facts and data also faces scrutiny. A report by the United States Office of the Director of National Intelligence (ODNI) noted that "countering faith with facts does not convince those who are radicalized or in the process thereof. The USG and its proxies must speak to their values and grievances, or otherwise redirect their attention".[22] A similar review by the United Kingdom's Institute for Strategic Dialogue (ISD) noted a similar recommendation for governments to also factor in the emotional appeal of some terrorism narratives and messaging to a target audience.[23]

While the world grapples with the challenges of formulating and measuring the effects of CT strategies and initiatives, the rapid rise and size of the so-called Islamic State (ISIS) presents a glaring gap between threat and response. Research shows that over 40,000 foreigners from 110 countries flocked to Iraq and Syria to join the group.[24] The unprecedented global mobilisation of foreign fighters to ISIS has been largely attributed to the group's considerable media and online presence and its successful leveraging of both traditional media and new media to its advantage. The terrorist group's 'multidimensional communications strategy' attracted widespread traditional media attention, while also making sure the group was heavily present on social media.[25] ISIS' communications strategy clearly translated into tens of thousands of foreign recruits willing to engage in violence, increasing the threat to innocents worldwide and to frustrating CT efforts against it.

A stark example of the evolving interplay between media and terrorism exists in the New Zealand mosque attacks of 2019. The terrorist broadcasted his actions live on the social media platform, Facebook, as he killed 51 worshippers. Around 200 people are believed to have watched the event live by the time the video was reported, about 12 minutes after the shootings ended. By the time the video was removed from Facebook around 4,000 people are believed to have watched it. In that time, many attempts were made to spread the violent content.

---

19 Glazzard, *Losing the Plot*.
20 Ferguson, *Countering violent extremism.*
21 UNSC Counter-Terrorism Committee Executive Directorate, *CTED Analytical Brief.*
22 ODNI, *Applying Private Sector*.
23 Briggs and Feve, *Review of Programs*.
24 Barrett, *Beyond the Caliphate*.
25 Ingram, *An analysis of*.

Within just the first 24 hours, Facebook blocked 1.4 million attempts to upload the video and remove a further 300,000 successful uploads. This attack was significant in many ways. It highlighted the futility of governments' and corporations' attempts to restrict the broadcast of live terrorist propaganda. It further highlighted that mass social media channels can simply be a launch platform for material to jump to less controlled websites or websites sympathetic to the terrorists' cause. New Zealand's Prime Minister reacted by framing social networks providers as "the publisher not just the postman".[26] Consequently, social media network providers face a difficult choice: either develop means for stopping real-time broadest of terrorist propaganda, currently technically impractical, or to stop providing a live broadcast service.[27]

The sudden and expansive rise of ISIS and the terrorist attack in New Zealand have reinforced the view that media and communications can and should be more aggressively leveraged in CT responses. Further, seemingly opposing ideological movements, like Salafi-jihadist inspired terrorism and white supremacy and far-right inspired terrorism often feed off one another's rhetoric and violence to advance their separate ideologies creating an additional level of complexity. Contemporary terrorist actors clearly recognise the power of media and communications in realizing their objectives and most experts advocate a role for media and communications in CT strategies and practices. The challenge lies in identifying what works. The available literature is rich on the matter of *how* terrorists use traditional and new media, including for propaganda, radicalization, recruitment, fundraising, communications, and operations.[28] Less apparent is evidence to explain *how* their use and exploitation of media leads to violent action and *what* serves as an effective government response. Further still, evidence is unavailable on whether government actors, especially from the security and military sectors, are best suited to lead communications-based responses to terrorism (CVE, counter-narratives and counter-messaging), especially those intended to change behaviours in groups and individuals. The first question for NATO, therefore, is: to what extent is the organisation required or capable of operating in the media domain of CT?

The vast focus on counter-narratives and counter-messaging in terrorism discourse today should not distract NATO and host governments from critical communications functions. Brigitte Nacos, an expert on media in terrorism and CT, makes several recommendations that governments should consider when managing terrorism crises. Many of these are of particular relevance to this chapter: she notes the importance of providing the media with a steady flow of information during and after terrorist incidents; she recognises the important role of mass media especially, television and radio, as the most effective ways to reassure and calm the public in times of crisis; and, she notes the importance of mass media for enhancing and coordinating emergency efforts – especially informing the public on what to do and what not to do.[29] (Nacos, 2007). These recommendations highlight the importance of trusted messaging and communications in countering and responding to terrorism and how policies and practices should not lose sight of the importance of public information and emergency and crisis response communications as well as in deploying counter narratives.

[26] BBC, *Facebook: New Zealand attack.*
[27] Ashraf, *Terrorism and Propaganda*.
[28] UNOCD, *The use of the Internet*.
[29] Nacos, *Mass-mediated Terrorism.*

The importance of these communications functions should not be compromised by security actors stepping into nascent and unproven communications-based responses to terrorism that risk blowback and could potentially compromise trust, credibility and reputation of the military. By virtue of being a security actor, NATO should be alive to and avoid the risk that it automatically securitizes[30] a message, its medium and the intended audience.

Good Practices

This study found very few examples of good practices in terms of CT and the media, certainly in a military context. Those that exist, appeared to be successful in a limited sense in terms of time and the targeted audience. Those practices also suffer from blowback in terms of creating a misleading context within which CT operations can take place and also in terms of contaminating the long-term reputation of the military with the failures or errors of short-term political leadership. Good practice, almost by definition, can only continue to be effective if the conditions within which that practice is developed remain unchanged. The nature of the terrorist threat is evolving and so CT operations are also adapting. The nature of mass media is changing dramatically as is the relationship that various consumers of mass media have with it. Given these and other evolutions, it is unsurprising that few examples of good practices can be identified. However, this study does offer some principles which could be applied to future CT media strategies to improve their effectiveness. These come from both a military and a civilian context and are chosen for their possible adaption to the CT scenario.

Good practice has been defined for this work as a technique, an activity, a strategy, a methodology or approach that has been shown, through application and evaluation, to be effective/and or efficient in achieving a desired result. The few such examples that existed were evaluated by looking at what recent history can teach us about their success. How terrorists take advantage of contemporary channels including television, radio press and digital media was also considered. The relationship between conventional mass communications and online, especially social media, communications was explored to determine the increasingly interdependent nature of these two mediums. This approach allowed us to develop an understanding of the principles, which rarely change, and of the practice, which must adapt to a continually evolving threat and context.

Cristina Archetti, a scholar focusing on political communication, notes that when governments and policymakers seek to understand the terrorism and media relationship, they tend to seek the contributions of terrorism experts, noting "the result is that "our" security (and foreign policy) is being influenced by scholars who know very little about how to make sense of global mediated politics".[31] Consequently, this study considered non-military examples of communications principles or practices that might be adapted for a security or military context, lessons from public policy areas and other non-terrorism fields:

[30] In this context securitization means the politicisation of the idea of terrorism to the extent that extraordinary, disproportionate or inappropriate means may be used in countering it. In particular it means that CT messaging adopts polarised troupes that divide opinions around identity or belief systems (e.g., the West, democracy etc) rather than unite (e.g., using terms such as innocents, civilians and criminals) opinion in order to represent a united response to the threat. In simple terms, any message from NATO will be perceived as representing its power and political interests rather those of the recipients'.

[31] Archetti, *Understanding Terrorism.*

Learning lessons from public health campaigns: A study by RAND Europe, noting the relatively recent emergence of the field of CVE, identifies transferable lessons for CVE from the evidence-based health care movement, which has a much more robust evaluation capacity.[32] The public health field could prove to be an important space for CT practitioners to study successful and measurable government efforts to influence and change public behaviour. There are good practices which can be considered from successful public health campaigns, for example around vaccinations and inoculations, routine health screenings, and antismoking initiatives. Further, communications campaigns from this field can play a role in "promoting social cohesion, encouraging more inclusive participation in public discussion, and increasing knowledge." Kate Ferguson concludes that "the evidence-based healthcare movement has an established track record of using evaluation to develop practice".[33] Finally, public health communications specialists have learned the importance of messaging that does not stigmatize or securitize health matters in society or among communities. These approaches could significantly enhance the appeal and behavioural impact of CT messaging, especially amongst potentially hostile audiences.

Lessons from successful public-private partnerships, especially as relates to critical infrastructure: Another field relevant for CT practitioners is to review and apply good practices from other fields with long-standing public-private partnerships, especially relating to terrorism matters. RUSI's Florence Keen notes: "Notwithstanding inherent differences between the two sectors, there are clear benefits in taking lessons learnt from longstanding efforts on terror financing into account when developing a response to the online terrorist threat. This coordination is becoming even more critical with the integration of Communication Service Providers and the financial sector, as in the case of peer-to-peer payments conducted over social media platforms".[34] Using this proven model, NATO should consider establishing partnerships with appropriate Communication Service Providers. One of the differences between the two sectors is that while the West has a dominant influence over the global financial system and can 'enforce' compliance with terror finance regulations such as anti-money laundering (AML), it does not have influence over many large-scale social media platforms. Odnoklassniki (classmates), for example, is a Russian social media platform which is very popular in former Soviet republics and has been the app of choice for foreign terrorist fighters from those countries in recent years. Similarly, WeChat is a popular Chinese app with users across the globe. NATO should consider deploying its diplomatic influence to arrange cooperative agreements with Russian and Chinese social media platforms based on the principle of a united response to a threat that these countries have in common with NATO member states. Commonality of interest at the international level is already expressed through notable entities operating at the intersection between communications, technology and CT include the Global Internet Forum to Counter Terrorism (GIFCT) and Hedayah.

Community and local dimensions in many successful security-related campaigns: Community and local engagement remain critical components for any government hoping

[32] Baruch et. al., *Evaluation in an emerging field*.
[33] Ferguson, *Countering violent extremism.*
[34] Keen, *Public–Private Collaboration*.

to collaborate with communities in risk-reducing behaviours. Again, while CVE remains a relatively nascent field, there are other security or policy related areas to learn from. A 2019 report by the Homeland Security Operational Analysis Center notes: "Such community education and engagement activities have been an element of initiatives in the criminal justice (e.g., community policing efforts), public health (e.g., participatory research models, community-level interventions), and in substance abuse intervention. The breadth of examples across fields is vast".[35] This principle of community engagement has been central to most Counter Insurgency (COIN) strategies. While these strategies have failed to deliver success in recent military campaigns, this was largely because community engagement has not been effectively delivered. A media strategy that is common and effective across the full spectrum of conflict, including CT, and which has community engagement at its heart is essential to victory in any contemporary context.

Lessons from 'Madison Avenue': When seeking to leverage the power of media and communications in any campaign, governments and security actors should also consider applicable lessons and good practices from leading practitioners in this space, namely from lessons from advertising agencies and 'Madison Avenue':

While social media is still relatively new (Twitter launched in 2006), many of the best practices for using it are based on well understood marketing approaches. The first, and perhaps most important, lesson is that a social media campaign must be part of a broader marketing strategy, whether to sell more shoes of a particular brand or to convince at-risk populations not to engage in violent extremist behaviour. Thus, our recommended approaches for using Twitter must ultimately be tied to an overarching campaign that seeks to undermine extremism.[36]

Aligning any messaging campaign to wider strategic effects, including kinetic effects, of NATO's operational campaigns is an obvious and well-known principle but its implementation has tended not to deliver success, except in deception operations. The principle is discussed again in this chapter.

Lessons from individualised campaigns: Notwithstanding the sparse evidence of the effectiveness of initiatives to counter online extremism, good practices could be adopted from individualised campaigns. "In general, the best evidence for effectiveness comes from prevention campaigns that target individuals in the process of radicalizing".[37] In order to do that, in-depth knowledge of the narratives being deployed by particular groups in specific regions is essential in designing and deploying counter narratives aligned with appropriate local political and social policy information. Knowledge and expertise on those regional specifics continue to accumulate in international organisations and academia and so NATO should consider setting up an active library of these drivers of radicalisation, possibly within the NATO COE DAT.

---

[35] Jackson, *Practical Terrorism Prevention*.
[36] Helmus and Bodine-Baron, *Empowering ISIS.*
[37] Jackson, *Practical Terrorism Prevention*.

Military-Specific Considerations for NATO

One of the major challenges in CT operations is responding to allegations of or to the actuality of collateral damage or military mistakes. Failure to do so effectively can result in an advantage for terrorists. For example, airstrikes in Kunduz on 4th September 2009, where over 70 civilians were killed was responded to by the Taliban setting up an 'inquiry' which resulted in a report indicating an objective, critical and emotive approach impressing both at the national and, to some extent, at the international level. Other incidents involving civilian casualties have also tended to be responded to slowly by NATO forces, after detailed investigations have taken place. By that time any admission of failure or compensation is ineffective because the terrorists and others fill the information void with allegations of deliberate targeting and cover ups. To avoid such situations, some generals have responded by adopting an active, sympathetic and affective approach involving immediate condolences to the families of the victims and assurances of best endeavour to avoid similar mistakes. This approach also adopts the mantra "first with the news – good or bad"[38] as long as accuracy is not compromised, and "first with the truth." However, these good practices have not necessarily been maintained by all military leaders. Therefore, one of the good practices for NATO would be to consistently apply its existing good practice.

When President George Bush described al-Qaeda's motives for attacking the USA as "they hate our freedoms: our freedom of religion, our freedom of speech, our freedom to vote …"[39] he successfully displaced Osama bin Laden's narrative that "We attack you because you occupy our lands and steal our wealth." This misrepresentation of al-Qaeda's narrative strategically frustrated the terrorist organization. However, it has not been as successful in countering al-Qaeda's narrative in non-western parts of the world. Indeed, the very act of CT in the form of the Global War on Terror has legitimised al-Qaeda's narrative in many parts of the world. Furthermore, the very effectiveness of this misrepresentation of al-Qaeda's narrative as an existential and non-negotiable threat to Western values, rather than to Western interests, has indoctrinated many involved in military operations, constraining their ability to think more widely about the range of choices and operational courses of action available to their communication strategy. It is important, therefore, to have a mechanism whereby militaries involved in CT do not become victims of the propaganda of their own side.

In major CT related operations there is sometimes pressure to construct messages and actions to aid political objectives. For example, during the Iraq war the U.S. government needed to present the growing insurgency to publics as being a foreign fighter phenomenon rather than an organic uprising. A media strategy was devised which had the effect of painting Abu Masab Al Zarqawi as a major foreign (he was Jordanian) insurgent leader when at time he led a relatively small group. This greatly benefited him and al-Qaeda in terms of profile and it presented the West with a greater CT challenge in the long term as Zarqawi's reputation enhanced allowing him to sow the seeds of the so-called Islamic State years later. All media strategies must be considered in terms of the balance between short term gain and long-term impact.

---

[38] Votel, *Next in Line*.

[39] Washington Post, *President Bush Addresses*.

In the context of CT related conflict, it may be helpful to think in terms of one of Clausewitz' trinities: Peoples' passion, Political rationality and military judgement. All of these are mediated through communication, usually through the media. The overall responsibility for the conflict rests with political power and the military is responsible only for military judgement. Both communicate on the same topic with people and deliberately or otherwise impact on their passions. In recent conflicts involving CT, the division of responsibility has not been clear, and the military has tended to present or support political decision-making as well as speaking directly to the people of nations involved in the conflict. Bad political policy is blamed on political leadership. In NATO's democratic countries, responsibility for political mistakes tarnishes the leaders and parties involved and is usually punished by non-election, sometimes by political obscurity. NATO and its militaries are enduring institutions. If they mouth political policy that is subsequently revealed to be a mistake or even deliberately misleading, then they may continue to suffer reputational damage. While NATO member states' populations can understand the distinction between political responsibility and military implementation, most of the countries within which NATO operations occur do not have a political culture with such a distinction of responsibility. It would, therefore, be appropriate for the military to repeatedly communicate a neutral stance on CT policy matters and only explain the physical aspects of the threat and the military aspects of its CT responsibility through mass media.

Conclusion

This chapter recommends that the principle of 'Politics has Primacy' should be applied to CT media strategies so that they are subordinate to and aligned with the CT political narrative. There should be a clear distinction of responsibility and transparency of ownership between the narrative relating to political rationale and those targeting the 'people's passions,' from those that relate purely to military judgement. The military should avoid straying outside its area of responsibility. Further, Commander's Intent in military operations should be expressed in terms of "the Message I want to send is…" rather than in terms of a physical objective that might underpin the overall coercive or deterrent strategy i.e., "kill or capture." That way, media becomes a primary strategic objective rather than a Line of Ops in support of other objectives. As with other aspects, media ops should involve seamless coordination between tactical, operational, strategic and grand strategic levels of command. In a coalition situation, sideways alignment of objectives and methods between nations is equally important.

Effective messaging can change behaviour and perceptions, which can be difficult to reverse afterwards. It is therefore important to avoid being tempted by short term gain when it could lead to long term pain. This point is linked to the need to clearly differentiate between military and political messaging and their different areas of responsibility. In democracies when political power demonstrates failure, its reputation declines and it is usually replaced. The military is mostly an enduring institution whose reputation remains with it. Reputation is key in determining a military's coercion and deterrence capability and should not be contaminated by political failure. Militaries should defend their reputation during CT operations by making it clear, through the media, what the military is responsible for and what political leadership is responsible for.

It is important for militaries' message effectiveness for them to gain the reputation for being "First with the News" and "First with the Truth." The challenge for NATO CT commanders is to understand the principles and practices, outlined in this study, that have been successfully used by both militaries and commercial organizations so that they can effectively adapt them to a particular operational environment in order to deliver sustainable strategic success.

Bibliography

Archetti, Cristina, (2013), *Understanding Terrorism in the Age of Global Media: A Communication Approach*, (New York: Palgrave Macmillan).

Ashraf, Afzal, (2021), *Terrorism and Propaganda*, (London: The Edward Elgar Handbook of Political Propaganda).

Barrett, Richard, (2017), "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees", The Soufan Center, 31 October 2017, https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf. (Accessed 15 December 2020)

Baruch, Ben, Ling, Tom, Warnes, Rich, and Hofman, Joanna, (2018), "Evaluation in an emerging field: Developing a measurement framework for the field of counter-violent-extremism", *Evaluation*, Vol. 24, No. 4, pp. 475-495.

BBC, (2019), "Facebook: New Zealand attack video viewed 4,000 times" https://www.bbc.com/news/business-47620519. (Accessed 15 December 2020)

Berduygina, Oksana N., Vladimirova, Tatyana N., and Chernyaeva, Elena V., (2019), "Trends in the Spread of Fake News in Mass Media", *Media Watch*, Vol. 10, No. 1, pp. 122-132.

Briggs, Rachel and Feve, Sebastien, (2013), "Review of Programs to Counter Narratives of Violent Extremism: What Works and What Are the Implications for Government?", Institute for Strategic Dialogue, https://www.dmeforpeace.org/peacexchange/wp-content/uploads/2018/10/Review-of-Programs-to-Counter-Narratives-of-Violent-Extremism.pdf. (Accessed 15 December 2020)

Collins, Ben, Zadrozny, Brandy and Saliba, Emmanuelle, (2020), "White nationalist group posing as antifa called for violence on Twitter", *NBC News*, 02 June 2020, https://www.nbcnews.com/tech/security/twitter-takes-down-washington-protest-disinformation-bot-behavior-n1221456. (Accessed 15 December 2020)

Ferguson, Kate, (2016), "Countering violent extremism through media and communication strategies", Partnership for Conflict, Crime & Security Research, 2016, https://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf. (Accessed 15 December 2020)

Glazzard, Andrew, (2017), "Losing the Plot: Narrative, Counter-Narrative and Violent Extremism", *ICCT Research Paper*, 2017, https://icct.nl/app/uploads/2017/05/ICCT-Glazzard-Losing-the-Plot-May-2017.pdf. (Accessed 15 December 2020)

Graham, Katherine, (1986), "Safeguarding Our Freedoms As We Cover Terrorist Acts", *The Washington Post*, 20 April 1986, https://www.washingtonpost.com/archive/opinions/1986/04/20/safeguarding-our-freedoms-as-we-cover-terrorist-acts/4ab41319-95dc-43ab-b28e-2fe634c5fac1/. (Accessed 15 December 2020)

Helmus, Todd C. and Bodine-Baron, Elizabeth, (2017), "Empowering ISIS Opponents on Twitter". *RAND Corporation*, 2017, https://www.rand.org/pubs/perspectives/PE227.html (Accessed 15 December 2020)

Hoffman, Bruce, (2017), *Inside Terrorism*, (Third Edition), (New York: Columbia University Press).

Holmer, Georgia, Bauman, Peter, and Aryaeinejad, Kateira, (2018), "Measuring Up: Evaluating the Impact of P/CVE Programs", United States Institute of Peace Press, 2018, https://www.usip.org/publications/2018/09/measuring-monitoring-and-evaluating-pcve-programs (Accessed 15 December 2020)

Ingram, Haroro J., (2016), "An analysis of Islamic State's Dabiq magazine", *Australian Journal of Political Science*, Vol. 51, No. 3, 2016, pp. 458-477.

Jackson, Brian A., (2019), "Practical Terrorism Prevention: Re-examining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence", *RAND Corporation*, 2019, https://www.rand.org/pubs/research_reports/RR2647.html (Accessed 15 December 2020)

Jenkins, Brian Michael, (2012), "The New Age of Terrorism", in David G. Kamien (ed.), *The McGraw-Hill Homeland Security Handbook*, (New York: McGraw-Hill Education).

Keen, Florence, (2019), "Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes: What Can be Learnt from Efforts on Terrorist Financing?", RUSI, Global Research Network on Terrorism and Technology, Paper No. 1, 2019, https://rusi.org/sites/default/files/20190206_gifct_paper_1_keen_public-private_partnerships_web.pdf (Accessed 15 December 2020)

Kemp, Simon, (2020), "Digital 2020 October Global Statshot Report", DataReportal, https://datareportal.com/reports/digital-2020-october-global-statshot (Accessed 15 December 2020)

Marthoz, Jean-Paul, (2017), *Terrorism and the Media: A Handbook for Journalists*, (Paris: UNESCO).

Moonshot CVE, (2020), "Social Grievances and Violent Extremism in Indonesia: Exploring the appetite for psychosocial support among at-risk audience", December 2020, https://moonshotcve.com/indonesia-social-grievances-violent-extremism/. (Accessed 15 December 2020)

Nacos, Brigitte L., (2007), *Mass-mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism*, (Second Edition), (Lanham, Md: Rowman & Littlefield, 2007).

ODNI, (2015), "Applying Private Sector Media Strategies to Fight Terrorism: A Public-Private Analytic Exchange Program", https://www.odni.gov/files/PE/Documents/Media-Strategies.pdf (Accessed 15 December 2020)

The Washington Post, (2001), "President Bush Addresses the Nation", 20 September 2001, https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html. (Accessed 15 December 2020)

United Nations Office of Drugs and Crime (UNODC), "The Use of the Internet for Terrorist Purposes", September 2012, https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf (Accessed 15 December 2020)

UNSC Counter-Terrorism Committee Executive Directorate, (2020), UNSC Counter-Terrorism Committee Executive Directorate, "CTED Analytical Brief: Countering Terrorist Narratives Online and Offline", 2020, https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Analytical_Brief_Countering_Terrorist_Narratives_Online_and_Offline.pdf. (Accessed 15 December 2020)

Votel, James, (2019), "Next in Line to Lead al-Qaida", The CTC Sentinel (Vol 10), Combating Terrorism Center, 2019, https://ctc.usma.edu/wp-content/uploads/2019/11/CTC-SENTINEL-102019.pdf (Accessed 15 December 2020)

Wilkinson, Paul, (1997), "The media and terrorism: A reassessment," *Terrorism and Political Violence*, Vol. 9, No. 2, pp. 51-64

CHAPTER VII

GOOD PRACTICES IN INTEGRATING A GENDER PERSPECTIVE INTO COUNTERING TERRORISM

Zeynep Sutalan

Introduction

The aspect of Gender in terrorism and counterterrorism (CT)[1] is one of the most neglected areas in policy-making world, and also in academia. The need to address this issue stems from the fact that neglecting the different roles women play in terrorism creates security gaps since it creates deficiencies in the terrorist threat assessment, and thus insufficient CT and countering violent extremism (CVE)[2] programming. There are good reasons for this: in addition to being victims of terrorism, women can consciously and deliberately decide to join terrorist organizations and can become supporters, facilitators, recruiters, perpetrators and propagandists of terrorism. Together with recognizing the agential power of women in terrorism, it is essential to recognize that an increasing and meaningful inclusion of women both in the design and implementation of CT and CVE programming is key to success. Recognizing women's agency in terrorism and counterterrorism is also operationally effective. Equally important is the fact that it is an international legal responsibility in line with the Women, Peace and Security (WPS) agenda of the United Nations (UN) and its link to the CT and CVE efforts constructed with the relevant UN Security Council Resolutions.[3]

---

1 NATO defines 'counterterrorism' as "all preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals and property against terrorist threats and/or acts, and to respond to terrorist acts". See it in NATO Standardization Office (NSO), *NATO Glossary,* 35.

2 Countering Violent Extremism (CVE) or Preventing Violent Extremism (PVE) is neither defined by UN nor by NATO. United Nations (UN) underlines that it is the prerogative of Member States to define both 'terrorism' and 'violent extremism' in accordance with the international law in general and international humanitarian law in particular. Without getting into the trap of definition, UN provides practical approach to both countering terrorism under the *UN Global Counterterrorism Strategy* (See in United Nations General Assembly, UN Global Counterterrorism and countering violent extremism under *UN Plan of Action to Prevent Violent Extremism* [See in United Nations General Assembly, "UN Plan of Action to Prevent Violent Extremism", UN General Assembly Resolution, A/RES/70 674)On the other hand, OSCE defines CVE as "proactive, non-coercive actions to counter efforts by violent extremists to radicalize, recruit, and mobilize followers to violence and to address specific factors that facilitate and enable violent extremist recruitment and radicalization to violence." See in Organisation for the Security and Co-operation in Europe (OSCE), *Understanding Referral Mechanisms,* 7. Therefore, it is fair to view CT (coercive) and CVE (non-coercive) as complementary programs, CVE focusing more on the prevention of terrorism.

3 United Nations Security Council Resolution (UNSCR) 1325 (2000) on Women, Peace and Security (WPS) that the international community admitted the differential impact of armed conflict on women, girls and children,

It was not until the adoption of the United Nations Security Council Resolution (UNSCR) 1325 (2000) on Women, Peace and Security (WPS)[4] that the international community recognized the different impact of armed conflict on women, girls and children, and recognized the need to include women in building and maintaining peace and security. With this landmark resolution[5], the international community quest for a concerted effort to protect women against gender-based violence, and to empower women for conflict prevention, ensuring their equal role in peace and security building. Therefore, "the core of the WPS Agenda is about protecting and promoting women's rights in conflict and post-conflict situations, including the right to equal and meaningful participation."[6]

More than a decade later, the international community under the guidance of the UNSC underlined the link between "threats to international peace and security caused by terrorist acts" and the WPS issues with the Resolution 2122 (2013)[7]. In forwarding the WPS agenda, one of the milestone efforts to be noted is the UNSCR 2242 (2015)[8] which joined the WPS agenda together with the CT and CVE effort. With the Resolution, UNSC highly recommended Member States and the Counter-Terrorism Committee Executive Directorate (CTED) to adopt a gender-sensitive approach in all its activities. Within this framework, UNSC, UN Counter-terrorism Committee (CTC) and CTED underline that a gender sensitive approach to CT and CVE necessitates focus on: "(i) women and girls as victims of terrorism, (ii) women as perpetrators, facilitators, and supporters of terrorism, (iii) women as agents in preventing and countering terrorism and violent extremism, and (iv) the differential impact of counter-terrorism strategies on women and women's rights."[9]

The lack of a gender-sensitive approach generally in security and particularly in the field of counterterrorism does not mean that there are not any substantial efforts to overcome the predominant gender-blindness. Though not immune to deficiencies, there are certain practices that are widely referred to as good practices in the field of CT and CVE. Therefore, in regard to the successful practices in addressing the gender aspect of counterterrorism, this article utilizes three case studies: mother schools, female engagement teams and gender advisors. The idea is to highlight different roles women can play in regard to countering terrorism. With these case studies, three roles women can play in CT and CVE as preventers, counter-terrorists and change-makers are scrutinized in relation to three different levels of analysis, the local, operational and cultural-institutional levels.

---

and recognized the need to include women in building and maintaining peace and security. With UNSCR 2242 (2015) WPS agenda joined together with the CT and countering violent extremism (CVE) work.

4 S/RES/1325(2000).

5 Although UNSCR 1325 has been seen as the success of the feminist strife and regarded as a good feminist work, for some feminist-pacifists and post-structuralist feminists, the resolution does not openly question and/or defy the present power structures and the war system and therefore includes inherent strategies of masculinized militarization. For more on the post-structuralist feminist approach to the UNSCR 1325. See in Nikoghosyan, *Co-optation of Feminism*, 7-18.

6 Fink and Davidian, *Complementarity and Convergence*, 157-170.

7 S/RES/2122 (2013)

8 S/RES/2242 (2015)

9 UN Gender, Security Council Counter-terrorism Committee, https://www.un.org/sc/ctc/focus-areas/gender/.

Good Practices

The three cases discussed in this chapter as 'good practices' in terms of applying a gender perspective to countering terrorism (and also countering violent extremism) are widely referred to good practices in line with the positive feedback from the executers in the field. However, measuring success in terms of which policy and programmes perform well in CT and CVE is a matter of dispute due to the lack of scientific tools for measurement. As stated by Fionnuala Ní Aoláin, UN Special Rapporteur on Counterterrorism and Human Rights: "… there is little or no robust monitoring and evaluation of such programs and practices".[10] In this respect, despite their gains, a closer, more critical look at these practices will bring us to a place where there is a need to rethink 'what good practice is, at the expense of what and/or whom'.

Women as Preventers: MotherSchools

Women's potential to prevent terrorism or violent extremism that leads to terrorism has been acknowledged specifically in relation to their roles as mothers. Therefore, motherhood has started to be viewed as 'the first line of defence', because mothers are able to recognize the behavioural changes[11] in the family members (husbands, sons and daughters) which may stem from radicalization and assist in intervening in that radicalization before the subject makes the transition to terrorist action. In this respect, women as mothers are thought to have unique potential to contribute in building resilience in the community.[12] According to Edit Schlaffer "… they *(mothers of terrorists)* already speak the language of security. After many of these conversations with mothers across the globe, I realized that they are on the forefront of a new security paradigm. They need to be the building blocks for a bottom-up security approach."[13]

The MotherSchool Model[14] was developed in 2008 by the Women Without Borders (WwB) and Sisters Against Violent Extremism (SAVE)[15]. It is, therefore, a civil society initiative, the value of which has been recognized widely by the international community. The pilot programming took place in India, Pakistan, Tajikistan, Indonesia, Nigeria and Tanzania. The project was based on the assumption that women, in line with their innate

[10] Aoláin, *Why Preventing?*

[11] The changes in behaviours might include becoming short-tempered, anxious, unsocial, isolated as well as leaning to violent manifestations, supporting extremist ideologies, criticism of other family members who are thought to be living or thinking in the 'wrong' way.

[12] Schlaffer and Kropiunigg, *A New Security Architecture*, 54-75.

[13] Schlaffer, *Mothers*.

[14] The model is based on an applied research study entitled "CSn Mothers Challenge Extremism?" by the WwB Founder and Executive Director Dr. Edit Schlaffer and WwB Research Director Professor Ulrich Kropiunigg, The three-year study focused on the attitudes of mothers, their perceptions and experiences about violent in Pakistan, Palestine, Israel, Nigeria, and Northern Ireland. See Women Without Borders, *Mothers for Change*, and Schlaffer and Kropiunigg, *Can Mothers?*

[15] There are two other related projects by SAVE and WwB called 'Mothers MOVE!' (Mothers Opposing Violent Extremism) and 'Witness in History' (about victims of terrorism) projects. See in http://womenwithoutborders-save.blogspot.com/p/mothers-move.html and http://womenwithoutborders-save.blogspot.com/p/witness-of-history.html

maternal instinct, were able to identify radicalization and were also willing and able to fight against it. "The central components of the MotherSchools curriculum are building confidence and self-esteem, increasing knowledge and reflection of parent-child dynamics, and delivering specific training in countering radicalization."[16] In line with the increasing challenge of foreign terrorist fighters, the program is being adopted to Europe, in Austria, Belgium, Germany, the United Kingdom and Macedonia.

But in addition to the benefits, the assumption that the model is based upon and similar assumptions in many other CVE contexts have been criticized for overestimating women's role as primary influencers in their societies or preventers of radicalization. Women might have multiple roles as mothers, wives and sisters, but this does not necessarily mean that they are influential in preventing the radicalization of family members in the desired way. Though limited in number, comparative studies have revealed that the patriarchal structures display different characteristics in different contexts and thus differing roles and influence on the part of women. Therefore, the idea of 'context matters' has to be born in mind.[17]

UN Women raises concerns over the potential risk that MotherSchools presents in terms of promoting "a stereotypical view of women's role in society"[18]. A closer look at the rationale behind this initiative reveals that the practice itself is built on the gender stereotypes that portrays women's nature as peaceful and ignores the possibility that mothers themselves may be supporters of terrorism or they themselves might be radicalizers or recruiters.[19] According to Katherine E. Brown, such "maternalistic logic" is based on two perceptions: one sees women as peaceful, the other as domesticated. These perceptions place women in CVE efforts as the moderate pacifying subjects (rather than agents with unique identities, experiences or decisions) whose realized potential is to preserve the security of the state through eliminating the threats that may stem from the radicalization of family members.[20] Therefore, it is critical to acknowledge the different roles women can play in terrorism apart from being the mothers of potential and actual terrorists.[21]

In addition to strengthening mothers' parenting capabilities, UN Women recommends that the CVE programs like the MotherSchool should include the education of mothers as well as daughters and specific training programs that can endow these women with skills to generate income. [22]

---

16 Schlaffer and Kropiunigg, *A New Security Architecture*, 63.

17 For the similarities and differences of the patriarchal contexts in the cases of Bangladesh and Indonesia, see Gordon and True, *Gender Stereotyped*, 74-91.

18 UN Women, *Preventing Conflict*, 229,

19 Winterbotham, *Do Mothers?*

20 Brown, *Gender and Counter-radicalization*, 36-59.

21 For detailed discussions about women, gender and terrorism, see Sjoberg and Gentry, *Mothers, Monsters*; Sjoberg and Gentry, *Women, Gender*.

22 UN Women, *The Global Study*, 229.

Women as Counter-terrorists: Female Engagement Teams (FETs)

Following the US invasion of Iraq in 2003, as soon as the direct combat operations were over, tactical control points were established in line with the stabilization missions to search for and seize weapons and other materials that had been smuggled by the 'terrorists/insurgents'[23] in Iraq. However, there was a cultural sensitivity around searching women, and the terrorists utilized this fact smuggling weapons, money, drugs and other material. Concurrently, women were being recruited and used as suicide bombers. This became a significant threat for the US military personnel and to counter this threat, the US Marine Corps (USMC) developed the Lioness Program which was based on providing Search Teams who would search Iraqi women, staffed by female military personnel. The program also included the training of Iraqi security personnel to conduct proper search operations targeting women.[24] Then with a similar intent, Female Engagement Teams (FETs) were formed and deployed to Afghanistan, firstly by the USMC on an *ad hoc* basis in 2009; this was then emulated by the UK and eventually, based upon reported success, the concept was adopted by ISAF.

The formation and deployment of Female Engagement Teams (FETs) first in Iraq and then in Afghanistan was not unlinked to the search for a way out from the morass of irregular warfare, and in line with the doctrine of counterinsurgency (COIN)[25], which was predominantly about winning the support of the population reflected in the famous saying of 'winning hearts and minds of the people'. One renowned COIN expert, David Kilcullen, who served as an advisor to both General David Petraeus and General Stanley McChrystal, has stated:

> History has taught us that most insurgent fighters are men. But, in traditional societies, women are extremely influential in forming the social networks that insurgents use for support. Co-opting neutral or friendly women, through targeted social and economic programs, builds networks of enlightened self-interest that eventually undermines the insurgents. To do this effectively requires your own female counterinsurgents. Win the women and you own the family unit. Own the family and you take a big step forward in mobilizing the population on your side.[26]

---

[23] NATO defines insurgency as: "Actions of an organized, often ideologically motivated, group or movement that seeks to affect or prevent political change or to overthrow a governing authority within a country or a region, focused on persuading or coercing the population through the use of violence and subversion." See in AAP-06 Edition 2019, NATO Glossary of Terms and Definitions (Brussel: NATO Standardization Office, 2019), 68. NATO defines terrorism as: "The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives." See in AAP-06, 28. When one looks at the NATO definitions of both terms, there are similarities, but the main emphasis on the insurgency definition seems to be the gaining the support of population whereas in the definition of terrorism there might be, not necessarily, an objective of gaining control of the population. However, neither in theory nor in practice, there seemed to be differences between the two.

[24] Dunn, *Lioness Program.*

[25] NATO defines COIN as "comprehensive civilian and military efforts made to defeat an insurgency and to address any core grievances." See in AAP-06 Edition 2019, *NATO Glossary*, 34. When it comes to the differences between COIN and CT, despite being posited as two different strategic doctrines, the line between the two become increasingly blurred, and they are intertwined in the battlefield. Contemporary CT has already become more than traditional hard power responses. For a more detailed discussion about hard vs soft power in counterterrorism, see Stephen Harley at this volume, *Hard Power, Soft Power*.

[26] Kilcullen, *Twenty-Eight Articles*.

In regard to Kilcullen's claims about including women in a COIN (or CT) campaign as a female counterinsurgent or a potential female heart to be won in the targeted population was in fact about 'operational effectiveness'. Following the increasing attention the issue of gender attracted in line with the UNSCR 1325 and the resultant WPS agenda's adoption by the international community[27], there has been a tendency to link the strategy of FETs with the WPS agenda in terms of increasing women's participation in conflict prevention, but as put forward by Laastad Dyvik, "FETs should not be read as a 'feminist awakening' within the 'soldier scholar' vanguard of counterinsurgency theory."[28] FETs have neither been about realizing a feminist agenda nor about empowering women and realizing women's rights. The primary motivation behind was achieving force protection. NATO's experiences in integrating a gender perspective into NATO-led military operations are dominated by the lessons learned and good practices from ISAF in Afghanistan and KFOR in Kosovo, and these 'out of area' operations proved that it is operationally effective to include more women in terms of "better access to the local population, more popular support, better information, better situational awareness, and smarter interventions with less risks and better outcomes"[29]. Recent empirical research[30] elaborating upon NATO's adaptation to gender-mainstreaming has revealed that NATO military bodies have outpaced the civilian ones in adaptation. Heidi Hardt and Stéphanie von Hlatky proposed that this was mainly because military bodies perceived gender-related changes as 'operationally effective' and that the military's rigid hierarchical structure and obedience to orders enabled fast implementation and thus adaptation.[31]

The women-focused strategy of FETs evolved out of necessity for searching local women for hidden explosives and weapons. Later their roles as female operatives for body search was extended to gather intelligence and information via engaging with the women in the society. In order to get a chance to engage with women and develop friendship, FETs are tasked to provide mobile medical services for women and children in rural areas.[32] It was not only women that the FETs were expected to engage with, but also Afghan men since female soldiers were respected for being soldiers in addition to being women. Therefore, their being viewed as a 'third gender' enabled Afghan men to approach them as well. However, the question of why female soldiers were more approachable compared to the male ones is a critical question to be answered. Matthew Hurley also asks this question in his article where he elaborates the way new gender norms are normalized within NATO via the sharing of success stories.[33] He cites a case study from a NATO Gender Training Booklet on "How Can Gender Make a Difference to Security in Operations?" about a FET member having conversation

[27] It was in 2007 that NATO developed its first policy on WPS with its allies and partners in the Euro-Atlantic Partnership Council (EAPC). See in NATO Headquarters, *Women, Peace and Security.*

[28] Dyvik, *Women as 'Practitioners'*, 422.

[29] Marriët Schuurman, *NATO and the Women*, 6.

[30] Hardt and von Hlatky's research is based on a qualitative content analysis of an original dataset (created by themselves) of ninety-seven gender-related guidelines of NATO and interviews with seventy-one elites. See Hardt and von Hlatky, *NATO's About-Face*, 136-159.

[31] Ibid, p.137.

[32] McBride and Wibben, *The Gendering*, 199-215.

[33] Hurley, *Watermelons and Weddings*, 436-456.

with a male farmer in the Sangin district of Afghanistan in the mid-2010. Thanks to the rapport one of the FET members developed with the farmer, critical information about the location of IEDs and Taliban insurgents in the area were revealed.[34] There, Hurley underlines:

> The report concludes from this male/female interaction that: "Female personnel can work within stereotypes to exploit gender norms towards achieving a desired end". The "success" from NATO's perspective contained within the case study is obvious: information about the enemy was obtained and force protection increased. […] The key question that should be posed is: how was this conclusion reached and what precisely does it mean? The specific summary of the case study does not make it clear what stereotypes the FET member was working within and what gender norms she was exploiting in order to gain information from the farmer, other than being a woman developing a rapport with a man.[35]

Although FETs were not assigned a direct intelligence gathering role, FET members were expected to serve as an information collection asset, because it was believed that the local women had the information, and it could be made accessible to the FETs based upon their friendly relationship. In fact, as underscored by Sippi Azarbaijani-Moghaddam, this has always been confusion as to whether the FETs are intel collectors or not, since this was not explicitly defined and stated, mainly because seeing the women in the targeted population as a 'source of intel' holds the risk of endangering the security of these women.[36] As listed by Azarbaijani-Moghaddam, in the case of USMC FET in Afghanistan for the year 2011 the specific tasks ranged from engaging Afghan men and women to supporting the Government of Afghanistan (GoA) to achieve its national and international commitments to women rights. FETs were seen as enabler for COIN and envisioned to be the 'human face of ISAF' through performing the roles of acquiring the trust of local women and convincing them to use their influence to deter and prevent terrorism and insurgency.[37]Besides, "in spite of everything on paper there was no real institutional home or support structure for FETs within ISAF"[38].

The experience of FETs in Afghanistan has highlighted the fact that female soldiers have a deescalating effect since they were accepted by the Afghan men and women in the practice of body and house search. If the FETs functions had been restricted to that it would be much easier to assess their effectiveness in regard to deescalating effect, increasing credibility, potential gathering information and thus, contributing to force protection. However, ambitious goals and plans with vague tasks built on 'imagined advantages' and lack of institutional structure brought several problems in general impact evaluation, too.

In conclusion, the formation and deployment of FETs can be regarded as a good practice in a complex CT environment due to the justification of 'operational effectiveness'. Apart from that, it is also a valuable practice in terms of increasing women's involvement as

[34] NATO, *How Can Gender.*
[35] Hurley, *Watermelons and Weddings*, 447.
[36] Azarbaijani-Moghaddam, *Seeking out,* 14.
[37] Ibid, 10.
[38] Ibid, 13.

CT operators, because even if it is not about achieving gender equality in the military, the presence of women has a potential to regender the military in terms of disrupting dominant masculinities.[39] However, this should not keep us from asking critical questions in regard to femininities and operational effectiveness. In addition, we should also beware of instrumentalizing women for operational needs when positing FETs as an example of good practice and in meeting the requirements of the WPS agenda.

Women as Change-makers: Gender Advisors (GENADs)

One of NATO's fundamental efforts in implementing the WPS agenda turns out to be the Gender Advisors (GENADs)[40] appointed to NATO headquarters and operations. Marriët Schuurman, NATO's Special Representative for Women, Peace and Security in the Office of the Secretary General (2014-2017), considered GENAD positions within senior level military commands and Gender Focal Points (GFPs) within different branches of KFOR and ISAF as areas of progress in 2015.[41] The network of GENADs and GFPs has been created in both the civilian and military bodies of NATO at different levels. According to Shuurman, "this network aims to ensure that a gender perspective is integrated in the day-to-day work of all branches, with gender advisors reporting directly to the highest civilian and military leadership (from commanders to the Secretary General), thus having direct influence on strategic decision-making"[42]. In addition, NATO's establishment of a high-level position of Special Representative for Women, Peace and Security in 2012 and turning it into a permanent post in 2014 was regarded as a good practice by the "Global Study on the Implementation of the United Nations Security Council Resolution 1325", published by UN Women.[43]

According to Bi-Strategic Command Directive 40-1, which was adopted in 2009 and revised twice in 2012 and 2017, the GENAD's role is defined as providing advice on the implementation of the UNSCR 1325 and related resolutions "and the integration of gender perspectives including, but not limited to, operations/missions, crisis/conflict analysis, concepts, doctrine, procedures and education and training"[44]. Within this framework, GFPs are created to support and facilitate the role of GENADs in staff functions. Since NATO aims to integrate gender perspectives in planning, operations, missions, education and training as well as exercise and evaluation and gender mainstreaming into all NATO policies and programmes in all areas and at all levels, the GENADs have a critical role in the institutionalization of these efforts.

[39] See reference to Cockburn and Hubic, *Gender and the Peacekeeping*, 116; Duncanson and Woodward, *Regendering the Military,* 12.

[40] Based on the summaries of the national reports, it was identified that there are 697 GENADs in national armed forces of NATO members. Although these numbers inform us about the situation, it is not reflecting the whole picture since not all NATO nations or partner nations are reporting. It can be said that there is a decrease in the number of nations reporting since the year 2016. Summary of the National Reports of NATO members and Partner Nations to the NATO Committee of Gender Perspectives, 65.

[41] Schuurman, *NATO and the Women*, 2.

[42] Ibid, 3.

[43] UN Women, *The Global Study*, 258.

[44] Bi-Strategic Command Directive 040-001 (Public Version): Integrating UNSCR 1325 and Gender Perspective into NATO Command Structure.

GENADs has been an integral part of UN Peacekeeping missions since the year 1999 when they were first appointed to the mission in Sierra Leone, then in Kosovo and then in Timor-Leste. European Union followed suit and integrated the GENAD function into its Common Security and Defence Policy (CSDP) missions.[45] NATO's adoption of GENADs came after 2008. NATO GENADs were deployed to Afghanistan first to ISAF, then to Resolute Support Mission and then to KFOR. The institutionalization of the GENAD function was realized through the Bi-Strategic Command Directive 40-1 in 2009.

The research done by Megan Bastick and Claire Duncanson about the experiences of GENADs in NATO and partner militaries based on the reflections of 21 Military GENADs over a seven-year time period provides us with critical insight.[46] When GENADs in NATO were asked about their achievements, their answers had two dimensions, one internal-institutional and the other external-operational environment. Regarding the internal dimension, there was a tendency among those interviewed to see their contribution to changing the mentality of the military as a success. They mostly emphasized that there is a progressive development towards integrating and institutionalizing a gender perspective into the military and its operations, based primarily on the efforts of the GENADs. When it comes to the operational environment, they did not claim organized positive impacts on the lives of conflict-affected people. They emphasized that some progress had been achieved in terms of developing rapport with local women as well as influencing them towards joining the security forces, but defined them as 'small wins': but they were hoping for more in future. As highlighted by Bastick and Duncanson: "…Military Gender Advisors can be agents of institutional change, given at least basic institutional support. They can, as they reported to us, change mindsets on an individual level, initiating conversations about equality and discrimination, challenging colleagues as to their attitudes."[47] Change in established gendered institutions with hyper-masculinity like a military will not happen overnight. But even 'small wins' and 'incremental changes' necessitates recognition and further support.

Despite the acknowledgement of the potential of GENADs in terms of regendering military and society, there are several challenges they face, one of which is ironically the resistance from inside the military, making their jobs twice as hard as well as making for embedding gender diversity in the military all the more challenging. They do still suffer from lack of clarification of mandate, being burdened by additional responsibilities, difficulties in establishing their positions in the chain of command, insufficient pre-deployment training and lack of resources. Additionally, for the development of necessary skills to act as a GENAD, it should be borne in mind that advising the command level differs from advising the ministerial level. Therefore, gender advisors who are to provide assistance for the foreign defence ministry require different sets of skills as well as experiences from the ones who are to advise the command.[48]

---

45 Olsson et al., *Gender, Peace and Security*.

46 Bastick and Duncanson, *Agents of Change,* 554-577.

47 Ibid, 573.

48 Open Discussion in COE-DAT Online Workshop on Gender and Counter-terrorism: Enhancing Women's Role and Empowering, 22-24 September 2020.

Conclusion

The first and foremost element in integrating a gender perspective to into CT (and CVE) starts with seeing gender as neither synonymous with women nor with sex. It is about being men and being women. Seeing gender as a social construct, not missing its intersection with other social factors like race, religion and class, we need to learn to think beyond gender stereotypes which align men with rationality, aggression and violence and women with emotions, passivity and peace. Awareness of such gender stereotypes will help us to get rid of our gender-blind lenses and see the issue of political violence and terrorism from a broader perspective that recognizes the different roles women can play in terrorism (from victims to perpetrators) and counterterrorism (from preventers to change-makers). Better assessment of the terrorist threat with gender awareness will enable us to better tailor our CT (and CVE) policies and programs.

Meaningful inclusion of women in CT and CVE is a key to success. However, ensuring the participation of women in CT and CVE should go beyond increasing numbers of female soldiers as a force multiplication or having GENADs for just meeting the WPS commitments. When integrating women into CT, women should not be pigeonholed into certain posts such as GENADs or FET members, but should be decision-makers in CT and CVE design.[49] Throughout this article, the few roles women can and do play in CT as preventers, implementers and change-makers have been addressed by reference to MotherSchools, FETs and GENADs. These references as good practices are not yet fully-fledged, and there is a long way to go in integrating a gender perspective into CT and CVE policy development and implementation, but the small gains provide hope for re-gendering security responses to the terrorist threat.

Bibliography

Azarbaijani-Moghaddam, Sippi, (2014), "Seeking out Their Afghan Sisters: Female Engagement Teams in Afghanistan". *CMI Paper*. Bergen:CHR Michelsen Institute.

Bastick, Megan and Claire Duncanson, (2018), "Agents of Change? Gender Advisors in NATO Militaries", *International Peacekeeping*, Vol. 25, No. 4, pp. 554-577.

Brown, Katherine E., (2013), "Gender and Counter-radicalization: Women and Emerging Counter-terror Measures," in Margaret L. Satterthwaite and Jane C. Huckerby (eds.), *Gender, National Security, and Counter-Terrorism: Human Rights Perspectives*, (New York: Routledge, 2013), pp. 36-59.

Chowdhury Fink, Naureen and Alison Davidian, (2018), "Complementarity and Convergence? Women, Peace and Security and Counterterrorism" in Fionnuala Ní Aoláin, Naomi R, Cahn, Dina Francesca Haynes, Nohla Valjl (eds.), *The Oxford Handbook of Gender and Conflict*, (New York: Oxford University Press), pp. 157-170.

Duncanson, Claire and Rachel Woodward, (2016), "Regendering the Military: Theorizing Women's Military Participation", *Security Dialogue*, Vol. 47, No. 1, pp. 3-21.

Dunn, Lance Cpl. Nicholas M., (2009), "Lione**ss** Program 'pride' of the Corps", USMC News, Articles, March 13, 2009, California: US Marine Corps Air Ground Combat Center, 2009, https://www.29palms.marines.mil/Articles/Article/498488/lioness-program-pride-of-the-corps/. (Accessed 15 December 2020)

[49] See Sutalan, *Women in Terrorism*, 54.

Security Council Counter-terrorism Committee, "Gender" https://www.un.org/sc/ctc/focus-areas/gender/. (Accessed 15 December 2020)

Gordon, Eleanor and Jacqui True, (2019), "Gender Stereotyped or Gender Responsive? Hidden Threats and Opportunities to Prevent and Counter Violent Extremism in Indonesia and Bangladesh," *The RUSI Journal*, Vol. 164, No. 4, June 2019, pp. 74-91.

Hardt, Heidi and Stéphanie von Hlatky, (2020), "NATO'a About-Face: Adaptation to Gender Mainstreaming in an Alliance Setting", *Journal of Global Studies*, Vol. 5, No.1, pp. 136-159.

Harley, Stephen, (at this volume), "Hard Power, Soft Power and Smart Power: Civil-Military Challenges in CT"

Hurley, Matthew, (2018), "Watermelons and Weddings: Making Women, Peace and Security "Relevant" at NATO Through (Re)Telling Stories of Success", *Global Society*, Vol. 32, No. 4, pp. 436-456.

Kilcullen, David, (2006), "Twenty-Eight Articles: Fundamentals of Company-level Counterinsurgency", March 2006, https://www.pegc.us/archive/Journals/iosphere_summer06_kilcullen.pdf. (Accessed 15 December 2020)

Lackenbauer, Helen and Richard Langlais (eds.), (2013), Review of the Practical Implications of UNSCR 1325 for the Conduct of NATO-led Operations and Missions. Stockholm: FOI.

McBride, Keally and Annick T. R. Wibben, (2012), "The Gendering of Counterinsurgency in Afghanistan", *Humanity*, Vol. 3, No. 2, Summer 2012, pp. 199-215.

NATO Standardization Office (NSO), (2019), *NATO Glossary of Terms and Definitions*: *AAP-06* Edition 2019.

NATO, (2011), "How Can Gender Make a Difference to Security in Operations-Indicators", Version 2011, https://www.nato.int/nato_static/assets/pdf/pdf_topics/20120308_1869-11_Gender_Brochure.pdf. (Accessed 15 December 2020)

NATO, (2017), Bi-Strategic Command Directive 040-001 (Public Version): Integrating UNSCR 1325 and Gender Perspective into NATO Command Structure, 17 October 2017, https://www.act.nato.int/images/stories/structure/genderadvisor/nu0761.pdf. (Accessed 15 December 2020)

NATO, (2018), Summary of the National Reports of NATO member and Partner Nations to the NATO Committee of Gender Perspectives, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200713-2018-Summary-NR-to-NCGP.pdf. (Accessed 15 December 2020)

Ní Aoláin, Fionnuala, (2020), "Why Preventing and Countering Violent Extremism Law and Practice Failing a Human Rights Audit", *Just Security*, 28 April 2020, https://www.justsecurity.org/69899/why-preventing-and-countering-violent-extremism-law-and-practice-is-failing-a-human-rights-audit/. (Accessed 15 December 2020)

Nikoghosyan, Anna, (2018), "Co-optation of Feminism: Gender, Militarism and the UNSCR 1325", *Feminist Critique: East European Journal of Feminist and Queer Studies*, No.1, pp. 7-18.

Olsson, Louise, Martin Åhlin, Marielle Sundin, Anna Lidström (eds.), (2014), *Gender, Peace and Security in the European Union's Field Missions*, (Stockholm: Folke Bernadotte Academy), https://fba.se/contentassets/bcfe134c7ace454c964c1cf68f856474/fba_csdp_rapport_s5_web_141217.pdf. (Accessed 15 December 2020)

Organisation for the Security and Co-operation in Europe (OSCE), (2019), *Understanding Referral Mechanisms in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: Navigating* Challenges and Protecting Human Rights: A Guidebook for South-Eastern Europe. Vienna, https://www.osce.org/files/f/documents/7/4/418274.pdf. (Accessed 15 December 2020)

Schlaffer, Edit and Kropiunigg, Ulrich, (2015), "Can Mothers Challenge Extremism? Mothers' Perceptions and Attitudes of Radicalisation and Violent Extremism", (Vienna: Women Without Borders).

Schlaffer, Edit and Kropiunigg, Ulrich, (2016), "A New Security Architecture: Mothers Included!" in Naureen Chowdhry Fink and Sara Zeiger, Rafia Bhulai (eds.), *A Man's World? Exploring The Roles of Women in Countering Terrorism and Violent Extremism*, (Hedayah and The Global Center on Cooperative Security), pp. 54-75.

Schlaffer, Edit, (2016), "Mothers, the much needed, but missing ally for counterterrorism", UNESCO, 30 October 2016, https://en.unesco.org/news/edit-schlaffer-mothers-much-needed-missing-ally-counterterrorism. (Accessed 15 December 2020)

Schuurman, Marriët, (2015), "NATO and the Women, Peace and Security Agenda: Time to Bring It Home", *The Quarterly Journal*, Vol. 15, No. 3, Summer 2015, https://www.nato.int/cps/en/natohq/opinions_124032.htm?selectedLocale=en. (Accessed 15 December 2020)

Sjoberg, Laura and Gentry, Caron E., (2007), *Mothers, Monsters, Whores: Women's Violence in Global Politics*, (London: Zed Books).

Sjoberg, Laura and Gentry, Caron E., (2015), *Beyond Mothers, Monsters, Whores: Thinking About Women's Violence in Global Politics*, (London: Zed Books).

Sjoberg, Laura and Gentry, Caron E., (eds.), (2011), *Women, Gender, and Terrorism*, (Athens: University of Georgia Press).

Sutalan, Zeynep (ed.), (2019), *Women in Terrorism and Counterterrorism*, Workshop Report, Ankara, COE-DAT.

Syvik, Synne Laastad, (2014), "Women as 'Practitioners' and 'Targets': Gender and Counterinsurgency in Afghanistan", *International Feminist Journal of Politics*, Vol. 16, No. 3, pp. 410-429, https://doi.org/10.1080/14616742.2013.779139

UN Security Council Resolution, (2000), S/RES/1325, http://unscr.com/en/resolutions/doc/1325. (Accessed 15 December 2020)

UN Security Council Resolution, (2013), S/RES/2122, https://undocs.org/s/res/2122(2013). (Accessed 15 December 2020)

UN Security Council Resolution, (2015), S/RES/2242 http://unscr.com/en/resolutions/2242. (Accessed 15 December 2020)

UN Women, (2015), *Preventing Conflict, Transforming Justice, Securing the Peace: The Global Study on the Implementation of United Nations Security Council Resolution 1325*, http://www.peacewomen.org/sites/default/files/UNW-GLOBAL-STUDY-1325-2015%20(1).pdf. (Accessed 15 December 2020)

United Nations, (2006), *UN Global Counterterrorism Strategy*, UN General Assembly Resolution, A/RES/60 28, https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy. (Accessed 15 December 2020)

United Nations, (2015), *UN Plan of Action to Prevent Violent Extremism,* UN General Assembly Resolution, A/RES/70 674, https://www.un.org/counterterrorism/plan-of-action-to-prevent-violent-extremism. (Accessed 15 December 2020)

Winterbotham, Emily, (2018), "Do Mothers Know Best? How Assumptions Harm CVE". .London: Tony Blair Institute of Global Change, https://institute.global/policy/do-mothers-know-best-how-assumptions-harm-cve. (Accessed 15 December 2020)

Women Without Borders, "Mothers for Change", https://wwb.org/activity/mothers-for-change-5/. (Accessed 15 December 2020)

ISBN 978-605-74376-0-0