Defence Against Terrorism Review
Vol.3, No.2, Fall 2010, pp.13- 22

ISSN: 1307-9190

Cyberattacks Against Estonia Raised Awareness of Cyberthreats

Jaak AAVIKSOO
Minister of Education and Research, Estonia

Abstract: *NATO has just agreed on its first Strategic Concept since 1999. Cyberdefense and cybersecurity occupy a prominent position in NATO and her allies' strategic thinking, but they represent so much more than a new security problem. Growing cybersecurity problems are a fact of our irreversible and irresistible movement toward an ever more interconnected and information-based world.*

Keywords: *Cyberattack, Estonia, Cyberdefence, Cybersecurity, Cyberterrorism*

Introduction

In April 2007, Estonia experienced a coordinated and massive attack against government infrastructure, financial service providers and domestic media. These attacks, intended to destabilize the government and foment civil unrest, were conducted entirely in cyberspace. While not the first cyberattacks, they represented the most sophisticated and clearly politically motivated attacks to date, and have come to be known as a "digital Pearl Harbor." After the attacks, Estonia made a conscious choice to publicize the extent and nature of the attacks, start a policy discussion on the centrality of cyberdefense to security, and push our Allies in the direction of concerted action, doctrinal change, and cooperation. Since then, Estonia has been at the forefront of international debate on cybersecurity and cyberdefense.

Estonia feels the sting of cyberthreats particularly sharply. We are a highly connected and web dependent society; 98% of bank transactions go over the web and people use the Internet to pay taxes, access medical records, and even vote. We are also a small country with limited natural resources. Our economy is dependent on trade and connections with the outside world. Our experiences embody the strategic bind of all developed countries: interconnectedness, openness, and technological dependence constitute our strengths, but they also form an Achilles heel. Those who would challenge our societies, our values, our economic power or our military strength know to focus their efforts on this major chink in our armor. In my brief presentation, I will focus on how Estonia's strategic thinking has reacted to cyberthreats and how we must cooperate to secure cyberspace as a whole

In no small part as a result of these attacks, the last few years have been a period of growing awareness of the problem and new attention to concepts like cybersecurity, cyberdefense, cyberdeterrence, cyberterrorism and cyberweapons. The defense community is now moving from an awareness-building stage into an institution-building and doctrine implementation phase.

Why Cyber Matters

In the last three years, we have spoken much about how 'cyber' presents a fundamental paradigm shift in the global security dynamic. Cyberthreats epitomize asymmetry: they are inexpensive and easily developed, they neutralize the conventional military superiority and secure position of Western countries, and leave the world's most technologically advanced and networked societies most vulnerable.

Cyberattacks are cheap to launch, requiring only the cost of minimal hardware and manpower. The tools of cyberattack are widely available to both states and non-state actors, from organized crime to the disgruntled lone hacker. The source of a cyberattack can be difficult to determine, as a cyberattack can be routed through third parties and countries, co-opting networks unrelated to the attacker or target. In cyberspace, there are no clear distinctions between combatants and non-combatants. Civilian targets are both valuable and easy to attack.

Our societies' vulnerability extends beyond a mere threat to critical infrastructure. Information societies depend on trust and open communication. Undermine these, and you can spread panic, destabilize democratic governments, and destroy massive amounts of wealth. Cybersecurity and defense is often spoken of alongside other so-called 'new threats' like energy security, climate change, or population movements, but cyber is more than a security and defense problem, a change in the structure of our societies, economies, and relations. Instead of talking about cybersecurity and cyberdefense, we need to speak of security and defense as a whole in a cyberworld.

Demystifying Cyber: Similarities to Existing Security Challenges

These risks from cyberspace have led to a certain aura around questions of cyber-security and cyberdefense. I would like to demystify these terms and consider how we can and must adapt our existing institutions and solutions to function in a cyber-and-information world. We do not have the luxury of reinventing the wheel, nor do we need to.

Cyberattacks and dangers share fundamental similarities to more conventional threats. Ultimately, real people launch and order cyberattacks, using hard physical infrastructure such as servers, power

lines, and data connections located in real places. Cyberattacks are guided by calculations of self-interest and risk, either individual or collective. There is a gradient of threats and capabilities, from hackers to states.

My talk is broken down into two parts: in the first section, I will look at the risks to modern society as a whole that arise from cyberspace. I will recommend we adapt a comprehensive approach to cybersecurity that integrates domestic security thinking in every country and creates meaningful international cooperation. In the second section, I consider the narrower implications cyberattacks have for militaries, ministries of defense, and our defensive alliances. Over the course of 45 minutes, I hope to outline strategies for making our societies as a whole, our existing defenses, and our international cooperation more resilient to cyberattack and able to navigate the straits of 21st century security.

A Comprehensive Approach to Security, Making Us More Resilient

The Old Model: Defense and Security are External and Internal Threats

We tend to distinguish between security and defense problems. Our common sense tells us security problems relate to internal threats, while defense threats come from outside. Historically, this division has made particular sense for the United States, for whom two oceans have helped separate external threats from domestic security concerns. This division does not work in cyberspace.

Asymmetric Threats Like Cyber Require a Comprehensive Approach

Cyberthreats disregard borders. Oceans do not provide a natural barrier against ones and zeros. Any cyberdefense will inevitably entail mitigating the effect of potential attacks. Securing cyberspace is thus largely a question of societal resilience, and requires you to ask: are your institutions, agencies, private sector, individual users able to absorb and bounce back from shocks and attacks?

Cooperation and a Multisector Approach

Following our 2007 cyberattacks, we came to several key conclusions. We realized that the old dividing lines between domestic and international conflicts, defense and security problems, law enforcement and military solutions, public and private do not hold in cyberspace. No single ministry or department can handle what is simultaneously a problem of infrastructure, defense, law enforcement, commerce, and civil liberties. Furthermore, 85% of web infrastructure is in private hands. Therefore, 80% of cyber-attacks are launched against private companies, NGOs, and individuals.

These challenges mandated a multisector approach and cooperation with the private sector. We developed a National Cybersecurity Strategy, which we adopted in 2008. The strategy offers a common vision for all actors in society on how to reduce our vulnerability in cyberspace. The document envisages specific guidelines for government and the private sector, universities, NGOs and citizens. Our goal is to resolve decision-making ambiguities that arise during fast-paced cyberconflicts, divide responsibility so as to make optimal use of our limited resources, ensure that our entire webspace is secure by including the private sector in developing a high level of security standards, and instill a general cybersecurity culture.

The notion of good cybercitizenship is crucial. We believe that a precondition for securing cyberspace is that every owner of a computer, computer network or information system feels responsible for the expedient and prudent use of information and communications technology. We achieve such good cyberhygiene through both regulation and awareness campaigns. Simple steps like updating virus software and downloading files responsibly slashes the risk of identity theft, data loss, quickly-spreading viruses, and botnets. Consider if computer users in the US and Canada had employed better cyberhygiene, many of the attacks against Estonia in 2007 simply would not have occurred.

We have included cyberscenarios in our crisis planning and have conducted comprehensive exercises and tests of our systems that include all sectors of society. In order to constantly learn and adapt, we strive toward a culture of informal cooperation, openness to criticism and learning from previous errors.

We have also found an innovative solution to the difficulties of finding qualified manpower to tackle cyberdefense. We have created a 'cyber' division in our all-volunteer home guard. Should we be subject to another cybercrisis, we will have a large pool of IT specialists, programmers, and hackers to help carry out an effective defense.

Admittedly, Estonia's small size gives us flexibility. We can literally gather key players from all sectors of society into one room. The combination of our small size and early adopter approach to information technology make Estonia the perfect test-bed for experimenting with new approaches to cyberdefense and security. This is one of the potential areas of deepened US-Estonian cooperation I have discussed with my counterparts during this trip.

International Cooperation

Cyberspace is global and no country is a 'cyberisland.' Cybersecurity today is in the same phase of development as maritime security in the 18th century. Cyberattackers honor no flag or national border. The state still has a long way to go before achieving a monopoly on the use of force. If the ability to instantly cross borders gives cybercriminals and cyberattackers a measure of impunity, we have but one choice: to extend the long arm of law and order across borders.

There is growing international cooperation between experts and policymakers, and international best practices are starting to evolve. While informal cooperation is good, the current level of contact occurs on too *ad hoc* a level. This cooperation needs to be formalized.

Existing EU and NATO structures are a good place to start formalizing such relationships. Both need to adapt their chains of command and decision-making procedures to the contingencies of fast-paced cyberconflicts. NATO is the best place to address many high-end cyberthreats, but it cannot solve all problems. The EU, with its experience in institutionalizing civilian cooperation, is a natural player and partner for the US. Sadly, NATO and EU coordination problems only amplify existing coordination difficulties among civilian and military structures that work in parallel with little communication.

To combat both criminal and state-sponsored threats, we need better detection and analysis of attacks. The same sensor networks, libraries of malicious code, collaboration among cybersecurity

crisis management centers, and agreements with ISPs to allow access to potentially sensitive data in times of crisis that we need to deal with cybercrime will also allow us to defend ourselves against malicious politically-motivated cyberattacks. Civil-military cooperation is, as elsewhere, essential here.

The US has urged NATO to build a cybershield that would consist of a comprehensive network of sensors, response teams and analysts to identify and quarantine incoming cyberattacks against military and civilian targets. The more nodes such a network has and the greater its reach, the more it benefits all involved. This is a fundamentally sound idea that needs more fleshing out. Developing such defenses is one of Estonia's and NATO's priorities following the new strategic concept, one we hope to work very closely with the US on.

Ultimately, this cooperation cannot be limited just to EU or NATO countries, nor can we neatly divide up responsibility between different international organizations. For instance, all democratic countries have a joint interest in IT forensics capabilities that do not tread on civil liberties. Rather, our needs call for a real spirit of trust and cooperation.

On the level of cybercrime and 'hacktivism,' a legal solution is possible. Rooting out cybercrime and cyberattacks carried out by non-state actors is a good step toward securing cyberspace as a whole. Although cybercrime only makes up part of the range of threats from cyberspace, it is a domain of lawlessness that constitutes a threat to all states and to the global commons; limiting cybercrime is in everyone's interest. Countries outside of Europe should sign on to the Council of Europe's Convention on Cyber Crime. In addition to mandating cooperation, the convention also sets a standard for domestic legislation. The willingness of third countries to be a party to this treaty is good proof of whether the goodwill to tackle international cybercrime is there. International law is in this case a boon to everyone's sovereignty.

Law enforcement has its limits. We cannot always identify perpetrators. Pariah states offer safe haven to cybercrime and terrorism. Certainly, no amount of international law has thus far ended war as we know it. States will be willing to channel their considerable resources into using cyberweapons towards political and warlike ends. Thus, we also need solutions for dealing with cyberwar.

Thinking of Cyber Defense in a Conventional Defense Context

Example: A Crippling Attack Against the EU or US

Consider the following potential cyberattack: one day, the US or EU wakes up to find electrical power stations shut down; communication by phone and Internet disabled; air, rail and road transport impossible; stock exchanges and day-to-day bank transactions frozen; crucial data in government and financial institutions scrambled and military units at home and abroad cut off from central command or sent fake orders. The attack is particularly effective because it combines sophisticated cybertechniques with traditional spies who can bypass safeguards designed to isolate secure and critical networks and physically connect these to the internet. A recent report put the cost of orchestrating precisely such an attack at about 150 million lira and 750 people working for one to two years. This represents a fraction of the cost of carrying out such an attack using bombs and traditional sabotage, but still requires complex coordination and a long-term investment in manpower and resources. Such attacks remain the preserve of states and state-sponsored groups.

We Still Need Military Defense Thinking for Cyber-Conflicts

The importance of strong cybersecurity in ensuring national security and mitigating the effects of all levels of cyberattack has led many to use the phrase 'cyberdefense' and 'cybersecurity' interchangeably. We are seeing, however, that the state has not fully lost its advantages and superior power in cyberspace. Allow me, thus, to contradict myself: when we are dealing with a state-launched or state-sponsored attack, or when an attack threatens critical infrastructure or the stability of a society, we must adopt an explicitly defense-oriented paradigm.

Many Countries are Developing Terrifying Cyberweapons

The militarization of cyberspace is currently under way. A number of countries have acknowledged that they are developing 'cyberweapons' for offensive use. At this level of development, there is a strong offensive advantage that even the best cybersecurity cannot mitigate. Cyberattacks can be combined with the conventional and intelligence capabilities available to states, magnifying their impact. While not as terrifying as all-out nuclear war, cyberattacks can damage physical infrastructure, cause loss of life, and sow widespread fear and panic that can quickly destabilize networked societies. In short, full-scale cyberwar could bring modern life to a halt.

Arms Control and Deterrence are an Uphill Battle in Cyberspace

Unfortunately, the standard logic of arms control is greatly complicated in the case of cyberweapons. There is no single weapon to control. The damage from cyberattacks comes not from technology, but its coordinated and targeted use. Consider loading a government website on your browser – a completely legal, innocuous activity. Yet when networks of thousands of computers are directed to simultaneously and repeatedly access the same networks for hours on end, it becomes a coordinated cyberattack. Even in the case of clearly mischievous acts, like breaking into a website or inserting malicious code, the difference between a lone hacker testing his skills and a state-sponsored attack is one of degree and organization, not of kind. Furthermore, challengers to our security have every incentive to develop and field cyberweapons and little reason to abide by a 'cyberarms' control regimen.

We can never fully solve the attribution problem in cyberspace. Whereas the source of an incoming missile is easy to discern, cyberattackers can mask their tracks. Misattribution can raise tensions and escalate conflicts. The attribution problem is compounded by cyber militias and hacktivists who may receive training, direction and technical assistance from states, but do not follow orders or even reside in the state. Such hacktivists have played a role in nearly every major cyberconflict. For these reasons, credible arms control and deterrent regimens would currently be challenging to establish.

Developing a sensor network will help address these problems; so will good human intelligence. Even when attribution is impossible, we can still rely on an obligation to assist. Governments have an obligation to assist if an attack is routed through their country or perpetrated by an attacker located within their country. A failure to do so amounts to complicity in the attack, potentially in a manner similar to the Taliban's complicity in harboring Al Qaeda in Afghanistan.

Given man's history of conflict, we should not rely too strongly on the hope that destructive cyberconflicts will not occur. This sad fact reinforces the need for strong cybersecurity measures

to increase our resilience against cyberattacks. Such defenses also serve as a form of deterrence by denial, preventing potential aggressors from benefitting from cyberattacks. As the likelihood of malicious cyberattacks by a state or state-sponsored group does go up, we must give thought to how our collective defense and alliances will react.

How Do Collective Security Guarantees Apply to Cyberdefense?

There has been a great deal of hand-wringing over how collective security guarantees, particularly the North Atlantic Treaty and the EU's Lisbon Treaty, apply to asymmetric threats like terrorism or cyberattacks. Does collective defense apply when lines of code take the place of bombs and bullets? I would argue this is the wrong question to ask.

The decision to invoke NATO's Article V (or the EU's Solidarity Clause) should not depend on the type of weapon used or the identity of the attacker. Article V comes into force in the case of an armed attack (the EU Solidarity Clause is even broader). Neither specifies what constitutes an armed attack, nor should they: technology and military practice changed in leaps and bounds during the 20th century, and there is no reason to believe the 21st century will be any different.

Our primary criterion must be the type of damage caused. Did an attack cause a loss of life, large-scale economic destruction, or damage to infrastructure? Did it intend to? To account for cyberattacks, we need merely to maintain 'cyberequivalency' because an attack in cyberspace warrants a response equivalent to what we would do if the attack had used kinetic means.

NATO's Article 5 Innovation After 9/11 as an Example

NATO's reaction to the attacks of September 11 illustrates these points. Civilian aircraft were turned into dangerous weapons as a result of the intentions of the attackers and the choice of their targets. NATO declared that an attack that resulted in the loss of thousands of lives and massive material damage was grounds for invoking Article V, regardless of the means used. Furthermore, the North Atlantic Council invoked Article V on September 12, 2001, only a day after the attacks had occurred, and as the identity of the attackers was still being sorted out. What mattered was the fact of the attack, not the identity of the attackers.

Collective Security Works Because it is Flexible

The very strength of Collective Security guarantees lies in their flexibility, which allows them to adapt to changing circumstances while maintaining the promise of collective security. NATO in particular has adapted to a changing world for 60 years, and will continue to do so. We should not artificially tie our hands or restrict that strength.

Military Preparation

Issues in cyberspace will not simply supplant existing problems. We must see cyberspace as an additional military dynamic that will contribute to an already crowded 21st century battle space. US Deputy Secretary of Defense William Lynn put it best when he called cyberspace a new domain of operations alongside land, air, sea and space.

In addition to threatening civilian networks, cyberattacks can target military systems directly, taking weapons and communications systems off line. In sum, as the US Air Force Cyber Command's strategic vision states, controlling cyberspace gives you "the potential to achieve victory before a kinetic shot is fired."

We must therefore harden our militaries against cyberattacks. If our conventional military advantages are reduced to naught, we face a deep crisis of confidence in our security architecture. NATO and individual allies should see cybercapacities as a major priority in force renewal.

The battlefield of the future will be a mixed one, where cyberattacks complement kinetic attacks. Georgia's experiences in 2008, where sophisticated cyberattacks and a well-organized propaganda effort supplemented a conventional offensive, suggest that there is no clear division between asymmetric and symmetric, conventional threats. 'Cyber' is the inescapable future of all militaries, and of NATO.

Cyberdefense is an area where NATO as a whole is on board. Despite cutting billions from their defense budget, the UK's recent Strategic Defense and Security Review allocated GBP 650 M and attention to cyberdefense and cybersecurity. Numerous other European allies have gone through review processes and similarly concluded to devote far greater attention to cyberspace. This past weekend, both Angela Merkel and British foreign secretary William Hague delivered major addresses on cyber defense.

Cyber-Consciousness in NATO's SOP

To counter these risks, NATO as an organization needs to work cyber into its daily thought. Military exercises should take into account cyber risks, and conduct stress tests of critical infrastructure. NATO needs practical exercises that cover detecting and analyzing cyber attacks, reacting to potential cyber-Article 5 situations, and decision procedures in the case of such an attack. Such exercises will reveal current weaknesses and unresolved doctrinal questions. NATO also needs to ensure robustness in its lines of communication to each member state, in its command and control systems, and in its logistical abilities. I am hopeful we can translate the positive momentum from adopting our Strategic Concept into realizing these changes.

NATO is debating how much responsibility the Alliance should carry for protecting key civilian critical infrastructure. NATO cannot alone protect key civilian infrastructure. NATO should, however, take a lead role in creating uniform standards and policies. The

Our defense establishments also need a culture of welcoming dissent and well-intentioned criticism within the defense sector. Junior officers or government officials who raise concerns about cybervulnerabilities should not see those concerns and their careers sidelined. Rather, they need to be empowered to participate in solving these problems, and be given constructive forums for voicing concerns within the chain of command. A top-down institutional culture will not allow us the flexibility and adaptability we need.

NATO CCDCOE in Tallinn

Estonia has played a strong role in developing cyber thinking and readiness in NATO. The NATO Collaborative Cyber Defence Center of Excellence, located in Tallinn, is investigating the legal,

policy, civil defense, strategic and tactical ramifications of the issues I have been covering. We are bridging the gap between current thinking and the strategic and doctrinal clarity threats from cyberspace require.

Conclusion

Cyberthreats constitute a profound revolution in the nature of threats to peace and the functioning of 21st century economies, states, and societies. In dealing with these changes, we have drawn three conclusions:

- First, the challenge from cyberspace is not primarily a technical challenge, but a question of leadership. Will we properly leverage our capabilities, resources, and brains? Are we willing to challenge our preconceptions, study our weak spots, and test our systems in taxing exercises?
- Second, achieving cybersecurity requires a combined, multisector, comprehensive approach that focuses on building civil-military relations, cooperation with private enterprise, and educates the citizen.
- Finally, cybersecurity and defense require an increased level of formal and informal international cooperation. Where possible, we should adapt existing structures and agreements, including the Council of Europe's convention on cybercrime. When necessary, we should design new approaches.

At every step, we should rely on the strength of the NATO, the trust we share as allies, the values we hold dear.