Fall 10-17-2017

Benchmarking Estonia's Cyber Security: An On-Ramping Methodology for Rapid Adoption and Implementation

Ernest Wong
United States Military Academy, ernest.wong@usma.edu

Nan Porter
United States Military Academy

McKinnon Hokanson
United States Military Academy

Bing Bing Xie
United States Military Academy

Recommended Citation
Wong, E., Porter, N., & McKinnon Hokanson. (2017). Benchmarking Estonia's cyber security: An on-ramping methodology for rapid adoption and implementation. Proceedings of the American Society for Engineering Management 2017 International Annual Conference. E-H. Ng, B. Nepal, and E. Schott (Eds). Huntsville, AL.

Proceedings of the American Society for Engineering Management 2017 International Annual Conference
E-H. Ng, B. Nepal, and E. Schott eds.

BENCHMARKING ESTONIA'S CYBER SECURITY: AN ON-RAMPING METHODOLOGY FOR RAPID ADOPTION AND IMPLEMENTATION

Ernest Y. Wong*, Nan Porter, McKinnon Hokanson, Bing Bing Xie
United States Military Academy

ernest.wong@usma.edu

Abstract
In April of 2007, Estonia fell victim to a series of distributed denial of service (DDoS) attacks that crippled its government websites, email servers, media outlets, and banking system for nearly a month. Due to the devastating effects of these cyber attacks, Estonia took great efforts to strengthen its cyber security protocols. This research analyzes the reforms that Estonia has implemented in its domestic and foreign policies and attempts to determine if any of it systemic improvements can help to also bolster cyber security in the United States (US). The findings from this research are that Estonia's policy reforms in cyber security have been the most significant in areas that the US currently lacks. Domestically, Estonia has a cyber education program that significantly highlights awareness of the risks to its critical cyber infrastructure. Estonia has also promoted public and private partnerships to jointly analyze, assess, and defend itself against future cyber attacks.. In foreign affairs, Estonia has bolstered its relationship with allied nations in new ways and has synchronized its foreign policies to improve stakeholder engagement on cyber defense. The critical changes that Estonia has adopted and implemented throughout the past decade are what this research endeavors to recommend for the US to consider into its defense of the cyber domain. Furthermore, this research proposes an on-ramping methodology that helps to frame how an organization can more easiliy integrate new processes, practices, and procedures that have worked well for others.

Keywords
Cyber defense and security, cyber resiliency, on-ramping adoption and implementation framework

Introduction
After the collapse of the Soviet Union in 1991, the Republic of Estonia's technological capabilities were virtually non-existent. Beginning in 1992, an economic foundation established under the new Estonian Prime Minister allowed businesses to be created without substantial delay. By 1998, all Estonian schools had computers equipped in the classroom for their students. Soon afterwards, Internet access was considered a critical enabling infrastructure, and free Wi-Fi spread throughout the country and became the national standard. In 2007, Estonia became the first country to allow online voting in a general election. Today, Estonia is a world leader in technology and is considered one of the most wired countries in Europe (Davis, 2007).

On April 30th 2007, pro-Russian hacktivists showcased the devastating impact that cyber effects can have on the world. Never before had an entire nation become rendered completely impotent due to a cyber attack. As a result of this unprecedented attack, cyber warfare was quickly added into the military lexicon. No longer were cyber attacks merely a nuisance that only banks and e-commerce sites had to contend with; the 2007 Russian cyber attacks on Estonia showed to the world just how dangerous and deadly a cyber adversary can be and exposed just how vulnerable nations are to attacks in the cyber domain (Herzog, 2011). In spite of the calamity it suffered, Estonia has demonstrated considerable resiliency after this attack, and the nation has helped to spur a substantial amount of significant improvements in cyber defense. In fact, within the span of just one decade Estonia has transitioned into becoming one of the most advanced nations in cyber security and cyber defense. As cyber attacks directed against American citizens, campanies, and the government increase, it will prove advantageous to examine the measures that Estonia has taken following Russia's cyber attack towards advancing the cyber security posture of the US. By analyzing and benchmarking the Estonian cyber security strategy after its 2007 cyber attack, this research identifies key lessons learned that can be applied to improve the overall cyber security posture for all nations. Finally, this research proposes an on-ramping methodology that will help to better frame how any organization looking to adopt and implement processes, practices, and procedures that have worked well for others can do so more efficiently and effectively.

Background

As a result of a massive and sustained cyber attack on its information infrastructure by Russian hackers and in the aftermath of the very first cyber attack directly targeting the national security of a country, Estonia became one of the first countries in the world to adopt a national cyber security strategy (Czosseck, Ottis, & Taliharm, 2011). The 2007 cyber attack directed at computers in the Estonian government, schools, and national media left the country without a number of essential services for nearly a month. Although some of the attacks on its system merely consisted of vandalism on government websites, the most serious attacks resulted in a series of distributed denial of service (DDoS) that left the country without access to the Internet, telephones, bank accounts, and credit cards (Czosseck, Ottis, & Taliharm, 2011). However, in the aftermath of this cyber attack, Estonia has implemented a number of significant structural changes that make it a paragon for cyber security. Accordingly, this research shows how the US government can benefit greatly from by examining the creation of Estonia's cyber defense strategy and considering the adoption of key parts of this strategy for US cyber security.

Republic of Estonia's Cyber Security Policy

Estonia's *Cyber Security Strategy 2014-2017* currently guides Estonia's cyber security program and is an integral part of the nation's broader security strategy (Estonia, 2014). The document helps to highlight key developments, assesses cyber threats to the nation, and provides measures to manage these threats as part of a whole-of-government effort. This cyber security strategy is similar to the original plan that Estonia put in place immediately after the attacks in 2007, and it continues to promote efforts that enhance the nation's cyber security. The primary objective of this updated strategy is to increase cyber security capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace for its citizens. To do so effectively, this strategy outlines several sub-goals which include ensuring protection of information systems underlying important services, enhancing the fight against cyber crime, developing national cyber defense capabilities, managing cyber security threats, and promoting and synchronizing international cyber security policy (Estonia, 2014).

This cyber strategy also dedicates considerable resources on increasing its people's understanding of cyber vulnerabilities. Estonia's Police and Border Guard Board has been tasked with elevating the nation's awareness of cyber threats, and as a result, has created web-constables that educate its citizens on the security of the Internet and help protect its children and young people with their online presence (Estonia, 2014). In addition, this strategy encourages greater integration between the private, public and third-party sectors in order to promote a more comprehensive cyber security posture. This has resulted in the creation of the Estonian Defense League's Cyber Unit which is composed of cybersecurity and industry professionals who volunteer their expertise to improve the security of Estonian state agencies' information systems through coordinated exercises and testing of cyber defense solutions (Estonia, 2014). With Estonia's view towards enhancing relationships with allies and promoting international cyber security policy, partnerships have extended beyond traditional regional entities, such as NATO, the European Union, and the Baltic States; Estonia has created new forms of cyber cooperation such as the Freedom Online Coalition, the United Nations Group of Governmental Experts, and the Friends of the Presidency of the European Union in order to grow and synchronize mutually beneficial security policies that Estonia wants to promote (Estonia, 2014).

Linkages to the Cyber Security Goals of the US Department of Defense

In 2015, the US Department of Defense (DoD) published its updated cyber security strategy and placed cyber threats as the nation's number one strategic threat (US DoD, 2015). In this document, the US DoD outlines its three three primary cyber missions: 1) to defend its own networks, systems, and information; 2) to be prepared to defend the US and its interests against cyber attacks of significant consequence; and 3) if directed by the President or the Secretary of Defense, it must be able to provide integrated cyber capabilities to support military operations and contingency plans (US DoD, 2015). The US DoD document also includes a number of strategic goals which include: 1) build and maintain ready forces and capabilities to conduct cyberspace operations; 2) defend the DoD information network and data as well as mitigate risks to DoD missions; 3) be prepared to defend the US homeland and US vital interests from disruptive or destructive cyber attacks; 4) build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; and 5) build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability (US DoD, 2015).

As with in the Estonian strategy, the US DoD cyber strategy places considerable emphasis on international alliances and partnerships in order to bolster global cyber security against potential threats and states: "All three of DoD's cyber missions require close collaboration with foreign allies and partners. . . and [the US] seeks to build partnership capacity in cybersecurity and cyber defense, and to deepen operational partnerships where appropriate"

(US DoD, 2015). And based on the many other similarities and overlapping goals among these two cyber strategies, it appears evident that the US DoD has placed meaningful stock in learning from Estonia's experiences and is putting in place defensive measures that will help to prevent a cyber attack as devastating as the one inflicted upon Estonia from happening again.

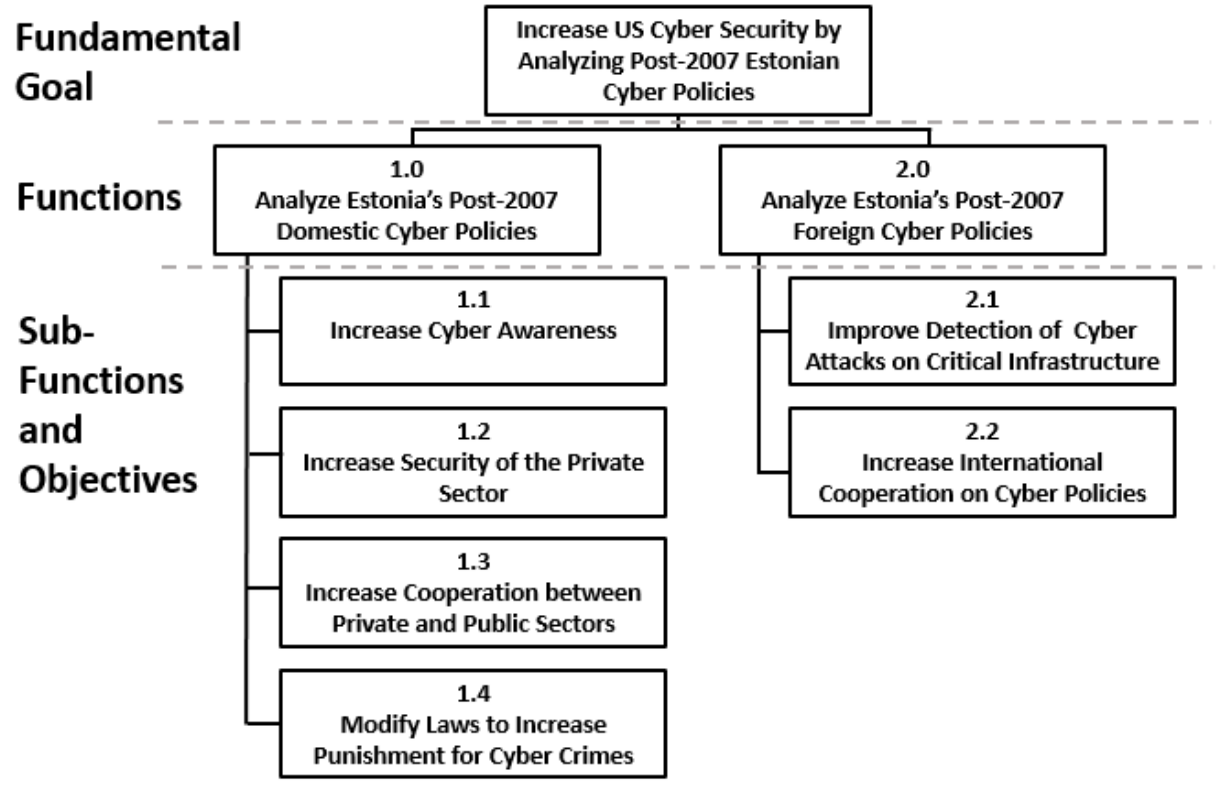
Methodology

While Estonia endured being without a number of critical services for over 22 days after the 2007 cyber attack, a number of security experts question whether the US, whose dependence on the cyber domain is arguably greater than Estonia's from a decade earlier, can withstand such a calamitous shock (Kaplan, 2016). "The network connectivity that the United States has used to tremendous advantage, economically and militarily, over the past 20 years has made the country more vulnerable than ever to cyber attacks," concluded the DoD Defense Science Board Task Force on Resilient Military Systems (US Defense Science Board, 2013). With cyber adversaries becoming more and more capable of conducting such attacks and with a computer network infrastructure that was built on inherently insecure architectures, the US has begun to realize that it must quickly ramp up and seriously improve its cyber defense capabilities. Studying, learning from, and emulating Estonia's cyber resiliency efforts can help to also reduce the US transition period in becoming prepared for a major cyber attack. This research begins first with structuring a functional hierarchy that helps define Estonia's cyber policies, then progresses to determining the relative values of Estonia's key cyber security improvement benchmarks, transitions next to a quantitative modeling process that helps to rank order cyber policies that have the most impact, and finally concludes with the introduction of an on-ramping framework that helps expedite organizational adoption and implementation.

A Functional Hierachy for Systematically Benchmarking Effective Cyber Policies

In order to benchmark the most critical and applicable portions of the *2014-2017 Estonian Cyber Strategy*, this research begins with a functional analysis to identify those system functions and system interfaces that have the greatest potential to improve the US cyber security posture (Parnell, Driscoll, & Henderson, 2011). The functional hierarchy depicted in Exhibit 1 highlights those areas and functions that this research conjectures would be most helpful in rapidly maturing the the US cyber strategy through emulating and learning from what Estonia has already

Exhibit 1. A Functional Hierachy for Analyzing Estonia's Post-2007 Cyber Policies



initiated for its cyber strategy. This functional hierarchy also provides this research with a clear plan of action and road map for analyzing the study's fundamental goal: how to increase US cyber security by evaluating the post-2007 Estonian cyber policies. This overarching goal, in turn, breaks down into two distinct functions—how Estonia has approached its domestic cyber policies and how it has navigated its foreign policies. Doing this permits the researchers to more easily compartmentalize the various interactions that define Estonia's cyber plan. From these two functions, the researchers identify six sub-functions and objectives that are detailed in Exhibit 1 and comprise the critical tasks which govern the direction of the scope, analysis, and modeling for this study.

Assigning the Relative Importance of the Sub-Functions and Objectives into a Swing Weight Matrix

Recognizing that not all value measures have equal importance, the researchers employ the swing weight methodology to quantify the tradeoffs between multiple objectives (Parnell, Driscoll, & Henderson, 2011). The matrix in Exhibt 2 shows how the researchers have come up with an assigned relative importance to each of the sub-functions and objectives in this study. The top side of the matrix defines the value measure importance and the left side defines the impact of changing the value measure range on the decision. Accordingly, this study arbitrarily scores 100 to the objective of Education and Awareness, located at the top left quadrant of the matrix, as the most important measure because it has the highest mission criticality and changes the most across its range of values, thereby providing the highest degree of variation. The arbitrary non-normalized scores—which are all below 100--for the remaining five other sub-functions and objectives are provided in Exhibit 2. What this matrix reveals is that this research has the Education and Awareness objective (with a score of 100) being weighted twice as much as the International Cooperation objective (with a score of 50) and being weighted five times as much as the Public and Private Sector Cooperation objective (with a score of 20). The basic concept of this method in determining weights is relatively straightforward with those objectives with more importance having higher scores than those with less importance (Parnell, Driscoll, & Henderson, 2011).

Exhibit 2. A Swing Weight Matrix for Quantifying Relative Importance of the 6 Sub-Functions and Objectives

Swing Weight Matrix		Level of importance of the value measure		
		High (Mission Critical)	**Medium** (Mission Enabling)	**Low** (Mission Enhancing)
Variation in measure ranges	**High** (Large capability gap)	Education and Awareness **100**	Security of Private Sector **70**	Public and Private Sector Cooperation **20**
	Medium (Significant capability gap)	Legal Changes **90**	Cyber Attack Detection **35**	
	Low (Small capability gap)	International Cooperation **50**		

Value Models to Quantify Each of the Sub-Functions and Objectives

In the next step of this study, the researchers construct value models for each of the sub-function and objective's value measurements. The equations provided for each of the value models in Exhibit 3 represent the best-fitting line for each of the 6 value measurements. Exhibit 4 concisely summarizes the key information about the quantitative value model from both the swing weight matrix as well as the 6 value models for each of the sub-functions and objectives.

Exhibit 3. Value Models and Functions for Each of the 6 Sub-Functions and Objectives

Exhibit 4. Key Information on the Swing Weight Matrix and Quantitative Value Models

Sub-Function & Objective	Measure Type	Value Shape	Swing Weight	Global Weight	Best Fitting Equation
1.1 Cyber Security Ed. and Aware.	Proxy	Convex	100	0.274	$y = 1.3393x^3 - 3.8929x + 2.8571$
1.2 Security of Private Sector	Proxy	Concave	70	0.192	$y = -2.6607x^2 + 31.95x + 4.1429$
1.3 Coop. b/w Pri. and Pub. Sectors	Proxy	S-Shape	20	0.055	$y = -0.1505x^3 + 2.5694x^2 - 0.7275x + 0.3968$
1.4 Legal Changes	Proxy	Concave	90	0.247	$y = -1.942x^2 + 27.848x - 3.0357$
2.1 Detecting Cyber Attacks	Proxy	Linear	35	0.096	$y = 10x$
2.2 International Cooperation	Proxy	S-Shape	50	0.137	$y = 0.013x^4 - 0.5845x^3 + 5.7465x^2 - 2.5926x + 0.2778$

Comparing US Cyber Security to Estonian Cyber Security and Recommending an On-Ramp Framework

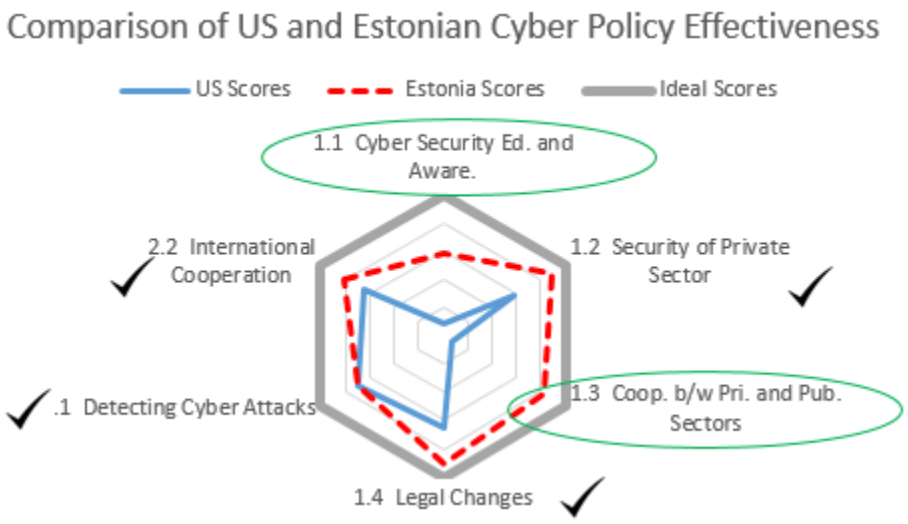
In the final step of this study, the researchers approximate the raw input data values to calculate how the overall US cyber policy weighted score compares against Estonia's score. As highlighted in Exhibit 5, the US overall weighted score of 45.14 is below Estonia's score of 76.95. While there may be concern that the US score falls below 50% of the Ideal Score, the researchers believe the overarching goal of this analysis is not to debate where the US falls in relation to other nations, but rather, to identify those key areas where the US can focus additional emphasis and resources to quickly improve its cyber security posture. The radar/web diagram in Exhibit 6 provides a more insightful

Exhibit 5. Comparison of Approximated US and Estonia Cyber Scores

Sub-Function & Objective	Global Weight	Best Fitting Equation	US Raw Data	US Score	Estonia Raw Data	Estonia Score	Ideal Raw Data	Ideal Score
1.1 Cyber Security Ed. and Aware.	0.274	$y = 1.3393x^3 - 3.8929x + 2.8571$	4	2.387479	8	15.734	10	26.81044
1.2 Security of Private Sector	0.192	$y = -2.6607x^2 + 31.95x + 4.1429$	2	11.00824	4	17.13978	6	19.18915
1.3 Coop. b/w Pri. and Pub. Sectors	0.055	$y = -0.1505x^3 + 2.5694x^2 - 0.7275x + 0.3968$	2	0.4392	8	4.49109	10	5.455441
1.4 Legal Changes	0.247	$y = -1.942x^2 + 27.848x - 3.0357$	3	15.54172	5	21.61339	7	23.85427
2.1 Detecting Cyber Attacks	0.096	$y = 10x$	7	6.712329	7	6.712329	10	9.589041
2.2 International Cooperation	0.137	$y = 0.013x^4 - 0.5845x^3 + 5.7465x^2 - 2.5926x + 0.2778$	5	9.046548	6	11.25921	9	13.91827
Total=	1.00		Total=	45.13551		76.94979		98.81661 *

*Does not sum to 100 due to rounding of raw data

Exhibit 6. Radar/Web Diagram Showing 2 Key Sub-Functions to Improve US Cyber Defense the Most

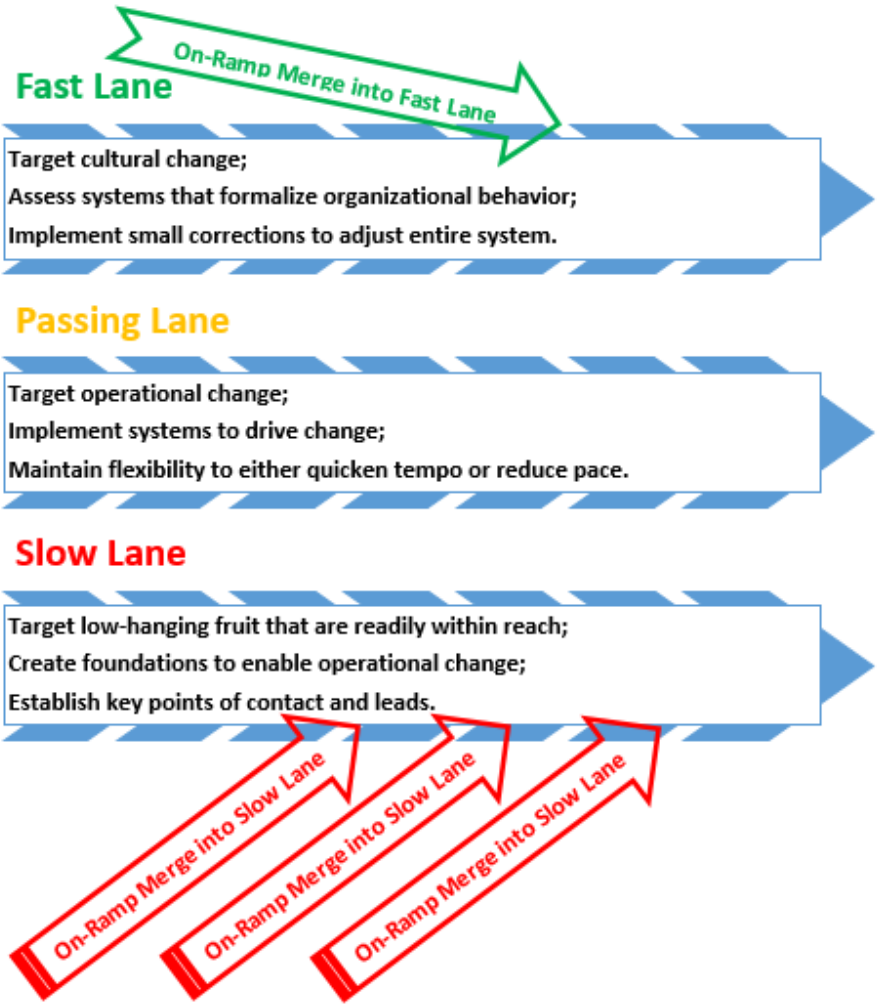


assessment beyond the calculated overall weighted scores. In order to move US policy towards the ideal perimeter, it ought to focus on improving in two key sub-functions and objectives: Cyber Security Education and Awareness and Cooperation Between Private and Public Sectors.

In order to help the US more rapidly adopt and implement policies and activities that address these two objective shortcomings, this research proposes that the US ought to adopt a "fast-lane" on-ramping methodology. Exhibit 7 depicts two methods that vehicles normally on-ramp on to an expressway: either via the fast-lane or via the more traditional slow/merge-lane. Because the US has already adopted and implemented a number of cyber polices that Estonia recommends, indicating that it has studied and is learning from Estonia's 2007 cyber attack, the US ought to have the capacity and capability to more readily implement additional measures to address its cyber defense shortcomings. The US has already implemented policies that target the low-hanging fruit most often seen in the slow-lane; instead it now needs to go after the harder policies that drive cultural shifts and organizational paradigm changes.

Increasing Education and Awareness as well as the promoting Public and Private Partnerships are difficult undertakings that will require a whole-of-nation strategy. But to ensure the nation is ready for a cyber event along the scale of Estonia's 2007 attack requires difficult and drastic change. The hope is that this research helps spur US policy-makers to think of a "fast-lane" on-ramp strategy as a viable option for the cyber resiliency of the entire US.

Exhibit 7. On-Ramping for Rapid Adoption and Implementation--Fast Lane vs Slow Lane On-Ramps



Conclusion

What makes Estonia supremely qualified to serve as an excellent benchmark for comparing cyber policies is that in April of 2007, it actually experienced a cyber-9/11 attack that fundamentally changed the way the entire nation approaches cyber security. This research acknowledges and affirms that the US has already adopted a number of domestic and foreign cyber security objectives that Estonia has proposed in its *Cyber Security Strategy 2014-2017*. However, this research concludes the US is deficient in two key objectives and recommends the US adopt a "fast-lane" on-ramping strategy that addresses how to better educate its citizens on cyber threats and promote the public and private partnerships that are critically necessary to ensure a cyber resilient nation. Although increasing awareness throughout the US will be difficult, this is a challenge that deserves consideration if the nation does truly wish to improve its overall cybersecurity posture and reduce the attack vectors available to cyber adversaries. Additionally, with the US private sector outpacing the public sector in developing new and novel ways for defending and operating in cyberspace, it is critically important that the US Government leverage as much technical and operational expertise from its own technology industries and companies. By focusing efforts on these two key areas, perhaps then the US

and its people will be more fully prepared to deal with cyber attacks as a normal part of being connected to the global economy rather than simply reacting to the consequences of a critical cyber event that takes the nation by surprise.

Acknowledgments

The authors would like to thank John Hennings, Paul Dufraine, and Dane Brown of the United States Central Command's Joint Cyberspace Center for sponsoring this research. The Systems Engineering Cadet Research Team (Team Estonia) is extremely grateful for their insights and guidance, and for taking the time to introduce our team to learning about cyber security at the global level. The views expressed in this paper are those of the authors and do not reflect official policy of the US Army, US Department of Defense, or the US Government.

References

Czosseck, C., Ottis, R., & Taliharm, A. (2011). Estonia after the 2007 cyber attacks: legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism*, 1(1), 24-34. Retrieved from http://www.irma-international.org/viewtitle/61328/

Davis, J. (2007). Hackers take down the most wired country in Europe. *Wired*. Retrieved from https://www.wired.com/2007/08/ff-estonia/

Herzog, S. (2011). Revisiting the Estonian cyber attacks: digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Parnell, G. S., Driscoll, P. J., & Henderson, D. L. eds. (2011). *Decision Making in Systems Engineering and Management, 2nd Edition*. Hoboken, NJ: Wiley.

Republic of Estonia Ministry of Economic Affairs and Communications (Estonia). (2014). *2014-2017 Cyber Security Strategy*. Retrieved from https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

United States Department of Defense (US DoD). (2015). *The DoD Cyber Strategy*. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

United States Deparmtent of Defense Defense Science Board Task Force on Resilient Military (US Defense Science Board). (2013). *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Retrieved from from http://www.dtic.mil/docs/citations/ADA569975

About the Authors

Ernest Y. Wong is a Military Intelligence Officer in the US Army who is serving as the Chief of Staff at the Army Cyber Institute and an Assistant Professor with the Department of Systems Engineering at West Point. He graduated from the United States Military Academy with a B.S. in economics, and he holds a M.S. in management science and engineering from Stanford University, a M.A. in education from Stanford University, and a Master of Military Science from the Mubarak al-Abdullah Joint Command and Staff College in Kuwait. He had the opportunity to work as a NASA Summer Faculty Fellow and has served in overseas deployments to Iraq, Kuwait, and the Republic of Korea. His research interests include disruptive innovations, cyber resiliency, and the application of systems engineering tools for resolving complex real-world problems.

Nan Porter, McKinnon Hokanson, and Bing Bing Xie were Cadets at the United States Military Academy who recently graduated and are serving as second lieutenants in the US Army. Nancy majored in Russian language and is now a Field Artillery Officer; McKinnon was defense strategy major and is an Infantry Officer; and Bing Bing majored in mathematics and is an Armor Officer. Together their capstone team researched how the US could best benchmark the cyber advancements that have taken place in Estonia for Lieutenant Wong's Applied Systems Design and Decision Making course.