SIMULATING POLITICAL AND ATTACK DYNAMICS OF THE 2007 ESTONIAN CYBER ATTACKS

Asmeret Bier Naugle
Michael L. Bernard

Cognitive Sciences and Systems Department
Cyber Engineering Research Institute
Sandia National Laboratories
PO Box 5800 MS 1327
Albuquerque, NM 87185, USA

Itamara Lochard

C4I & Cyber Center of Excellence
George Mason University
4000 University Drive, MS-485
Fairfax, VA 22030, USA

ABSTRACT

The Republic of Estonia faced a series of cyber attacks and riots in 2007 that seemed to be highly coordinated and politically motivated, causing short-lived but substantial impact to Estonia's cyber and economic systems. Short-term harm from these hybrid incidents led to long-term improvements and leadership by Estonia in the cyber arena. We created a causal model of these attacks to simulate their dynamics. The model uses the DYMATICA framework, a cognitive-system dynamics structure used to quantify and simulate elicited information from subject matter experts. This historical case study underscores how cyber warfare can be a major threat to modern society, and how it can be combined with information operations and kinetic effects to create further disruption. Given states' potential vulnerability to cyber attacks, a deeper understanding of how to analyze, prevent, defend, and utilize the aftermath of these for improvement to systems is critical, as is insight into the fundamental rationale of the outcomes.

1 INTRODUCTION

Beginning on April 27, 2007, Estonia was confronted with a series of coordinated cyber attacks. These, along with the simultaneous rioting and looting in the capital, Tallinn, have traditionally been considered as being triggered by the Estonian government's decision to move the Bronze Soldier of Tallinn, a World War II era Soviet monument, along with the bodies buried beneath, it from the capital's Old Town district to a military cemetery. However, additional field research and interviews conducted for this project demonstrates a broader strategy aimed at disrupting the Estonian government by a foreign state actor via an information operation as well as the presence of professional instigators were major contributing factors in these events (Estonian National Interviews 1-16 by I. Lochard 2016). Moreover, the timing, apparent coordination of the cyber attacks, and rioting indicate that they were highly organized (Tikk et al. 2010). Although these cyber incidents against Estonia were brief and relatively short-lived, they were disruptive to this high-tech, cyber-dependent country. Yet the events spurred Estonia's leaders to further strengthen their cyber systems and defense capabilities, helping them become one of the world's leaders in cyber defense.

We simulated this historical scenario for three purposes. First, to identify a hypothesized causal structure and sequence of events that may have led to the cyber attacks and determined Estonia's reactions to those attacks. Second, to gain insight into how different reactions and policies may have led to various outcomes. Finally, we hope that learning about this historical scenario can help us better

978-1-5090-4486-3/16/$31.00 ©2016 IEEE

understand potential future causes and impacts of hybrid cyber attacks, perhaps leading to better ways to anticipate, identify, defend against, and react to similar situations.

This article describes a model of the dynamics of the 2007 Estonian attacks. This model focuses on the dynamics of the cyber events, information campaign, and rioting, as well as defensive actions and decisions to strengthen cyber systems after the attacks. To simulate and assess these dynamics, we use a hybrid cognitive-system dynamics framework called DYMATICA (DYnamic Multi-Scale Assessment Tool for Integrated Cognitive-behavioral Actions), which quantitatively represents interactions between key actors in the defined system to indicate likely outcomes over time and enable rich exploration of results under a variety of conditions. DYMATICA assessments may provide both intuitive and non-intuitive outputs. The output of a DYMATICA simulation is intended to support existing assessments methods by providing insight into the causal interactions and influences that can affect outcomes of a situation.

2 THE 2007 CYBER ATTACKS ON ESTONIA

2.1 Background on the 2007 Cyber Attacks on Estonia

The Estonian government decided to move the Bronze Soldier statue and the bodies of fallen Soviet soldiers buried beneath it from the capital's Old Town district to a military cemetery in April 2007. The formal justification for the move was to provide a more appropriate burial ground. However, there was an additional security concern that the onset of ethnic-Russian protests at the statue in 2006 was part of a greater Russian strategy to assert control over former Soviet satellite countries. Similar events involving information campaigns, professional instigators, and rioting by ethnic Russians took place in 2004 and 2005 in Chechnya and Latvia, respectively. Prior to 2006, the Bronze Soldier in Tallinn had been a peaceful gathering place for ethnic Russians particularly on the 9 May Victory Day of Soviet Russia over Nazi Germany (Estonian National Interviews 1-16 by Lochard 2016).

Estonia declared its sovereignty from the Soviet Union in 1988 and gained independence in 1991. However, Russia had kept a relatively significant influence on Estonia despite the Baltic country's desire for autonomy and ethnic Russians comprise a significant portion of Estonia's population (25.1% as of 2015, according to Statistics Estonia (2015). The monument also depicted a World War II era Soviet soldier, which for many in the country symbolized Russia's continuing presence and influence. Estonia publicly announced the statue and fallen Soviet soldiers buried beneath it would be moved to a military cemetery six months in advance. However, the move date was close to the 9 May Soviet Victory Day against Nazi Germany. The timing was projected in social media, chatrooms, and in public statements by Russian officials as a racists, pro-Nazi stance by the Estonian people against ethnic-Russians which Estonians refute. When the statue was moved and the attacks commenced, the Russian government formally announced the Estonian government should step down. Both Estonian and Russian political factions were heavily invested in the outcome (Estonian National Interviews 1-16 by Lochard 2016).

The Estonian economy and contemporary culture are high-tech in character and functionality which appeared to render the country vulnerable to potential cyber attacks. When the Bronze Soldier of Tallinn was moved, rioting and looting erupted in Tallinn, followed by four phases of highly coordinated Distributed Denial of Service (DDoS) attacks that lasted through May 18, 2007. Video surveillance, local newspaper articles, and interviews demonstrate the role of foreign professional instigators involved in both the coordination and execution of the violence. In addition, there were multiple official reports of intimidation threats against government responders. The events were highly disruptive to the Estonian population, accustomed to generally low rates of violence and a very high dependence on cyber services. The "Estonian singing revolution" against the former Soviet Union from which it gained its independence was peaceful and the last riot in Estonia prior to 2007 took place on December 9, 1924 (Estonian National Interviews 1-16 by Lochard 2016).

Estonia had a relatively strong cyber defense capability at the time of the attacks (Ashmore 2009), so was able to quickly respond and mitigate the length of the outages. Cyber defenders used a variety of methods, and the United States, France, Finland, Latvia, NATO and others offered defensive assistance in riot gear which did not exist in the country prior to these events, as well as technical assistance (Estonian National Interviews by Lochard 1-16 2016). Estonia responded by further strengthening its cyber systems and strategies and has since become a world leader in cyber security. Most of their government, educational, social, medical, and economic services are now highly connected to the cyber domain. In addition, they are now known for their innovative use of security techniques and development of well-known technical software such as Skype and host NATO's Cooperative Cyber Defense Center of Excellence which runs the annual NATO Locked Shields exercise.

2.2 Conceptual Model

A causal loop diagram is a visual representation of the causal structure of a system commonly used in system dynamics modeling. We use these diagrams to scope our projects and models, as well as to come to a common understanding about our hypothesized causal system structure with our project team, subject matter experts, and other stakeholders. Creating a causal loop diagram can be considered conceptual modeling (Robinson et al. 2015). This causal loop diagram was built in an iterative process with (1) the project team, who conducted an extensive literature review on the topic, and (2) subject matter experts, who provided invaluable insight into what happened during the attacks, reasons for these occurrences, and likely motivations of the players.

To read the causal loop diagram, first note that each text block represents a variable. Arrows represent causal connections between variables, with each arrow pointing from the causal variable toward the affected variable. Each arrow has a + or – sign next to it, indicating either a positive relationship, in which the variables are likely to change in the same direction, or a negative relationship, in which the variables change in opposite directions, respectively. Some, but not all, of the feedback loops are also labeled. A (-) label indicates a negative, or balancing, feedback loop, which will tend to pull the system toward some equilibrium over time. A (+) label indicates a positive, or reinforcing, feedback loop, which will tend to move away from equilibrium over time and may result in vicious cycle behavior.

The upper left hand corner of the causal loop diagram for this model (figure 1) shows how the movement of the Bronze Soldier of Tallinn in combination with the information campaign may have aggravated hostility, ultimately leading to cyber attacks and rioting. The monument was a symbol that Russia retained power and continued presence in Estonia, a sentiment resented by many Estonians. It was believed by Estonians that Russian information operations in Chechnya and Latvia in the preceding years lead to similar protests and rioting as an effort to assert Russian control. As a result, the Estonian government issued a series of official warnings six months in advance to Estonians and others that it planned to move the monument and bodies beneath it.

However, the proposed date of the move was heralded in an information campaign in Russian as an indication of Estonian racism since it was close to the Soviet Victory Day over Nazi Germany. This amplified hostility by ethnic Russians toward the Estonian government. The level of discontent among the attackers (since there has been no official attribution, we will refer to this group generically) against Estonia increased, and had ample time to foment during approximately half a year of planning prior to the 2007 events. Additional information campaign on social media and chatrooms in Russian fostered both cyber incidents and riots. They also ensured through this planning process that there was plausible deniability regarding their participation (Estonian National Interviews by 1-6 Lochard 2016).

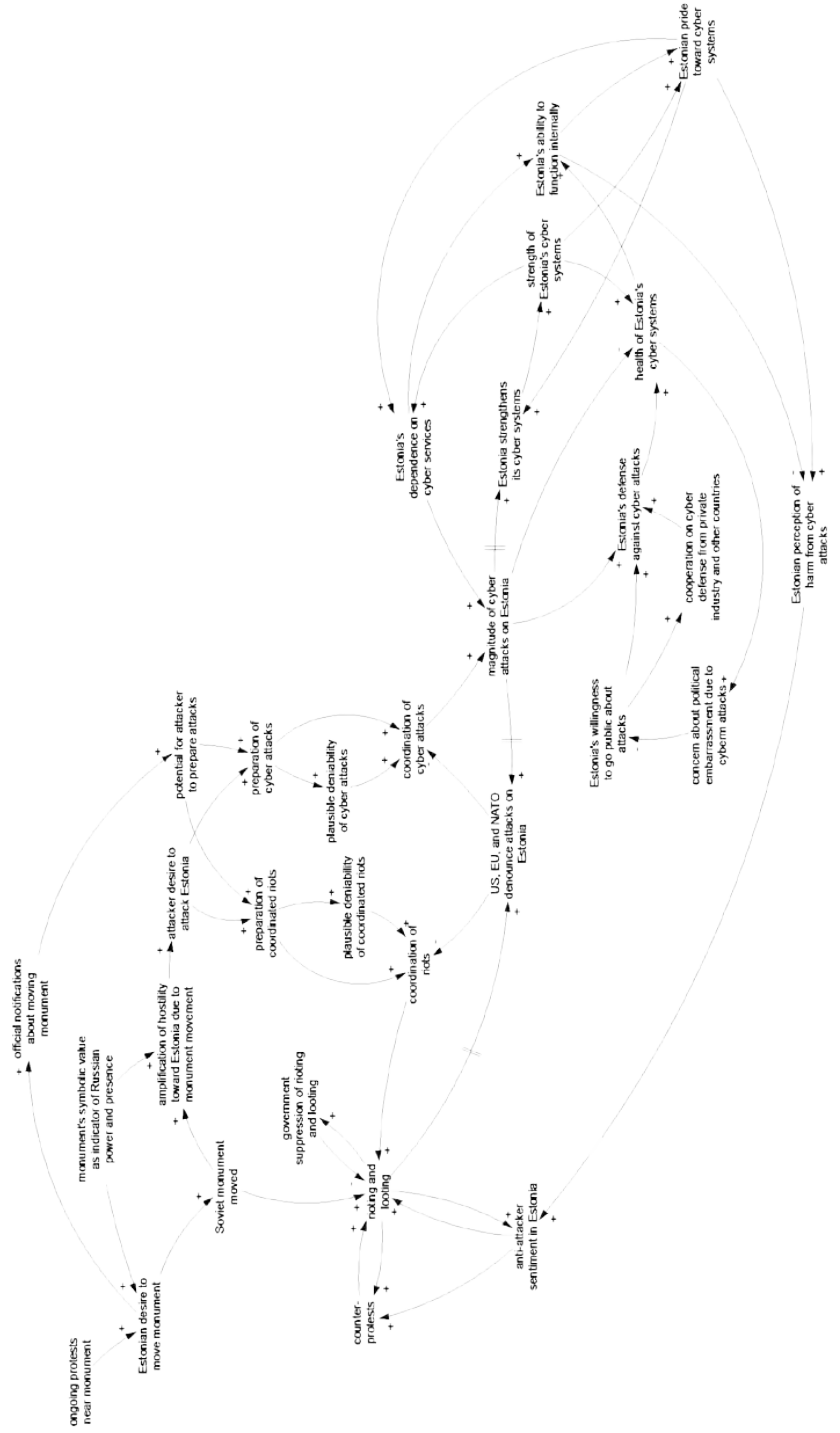
Estonian pride toward cyber systems
Estonia's ability to function internally
strength of Estonia's cyber systems
health of Estonia's cyber systems
Estonia's dependence on cyber services
Estonia strengthens its cyber systems
Estonia's defense against cyber attacks
cooperation on cyber defense from private industry and other countries
Estonian perception of harm from cyber attacks
magnitude of cyber attacks on Estonia
Estonia's willingness to go public about attacks
concern about political embarrassment due to cyberm attacks
coordination of cyber attacks
preparation of cyber attacks
plausible deniability of cyber attacks
potential for attacker to prepare attacks
US, EU, and NATO denounce attacks on Estonia
attacker desire to attack Estonia
preparation of coordinated riots
plausible deniability of coordinated riots
coordination of riots
official notifications about moving monument
monument's symbolic value as indicator of Russian power and presence
amplification of hostility toward Estonia due to monument movement
government suppression of rioting and looting
Soviet monument moved
rioting and looting
anti-attacker sentiment in Estonia
Estonian desire to move monument
ongoing protests near monument
counter-protests

Figure 1: Causal loop diagram describing the hypothesized structure of the scenario.

Riots and looting (described in the lower left part of figure 1) were believed to have been coordinated by professional foreign instigators from Russia. This led to some counter-protests, which in turn increased the intensity of the attacker-coordinated riots. The Estonian government actively suppressed the riots and looting using riot gear sent from neighboring countries and law enforcement, which helped to temper the rioting activity. Ironically, the rioting and looting increased negative sentiment about the attacker groups among the Estonian population as well as the ethnic Russian population residing in Estonia. This was evident in the attackers' inability to continue the violence in other Estonian cities despite a major leaflet campaign and chatroom effort to do so (Estonian National Interviews 1-16 by Lochard 2016).

Along with the rioting and looting, a series of coordinated DDoS cyber attacks were quite effective at crippling some of Estonia's important cyber capabilities by overwhelmed them. Though it was reported that major disruptions in both public and governmental services occurred given Estonia's high connectivity, relatively little disruption occurred and most banking systems remained functional with periods of occasional outages. However the combined effect of the kinetic and cyber attacks was perceived as an attempt to overtake the country. (Estonian National Interviews 1-16 by Lochard 2016). In response, Estonia launched defensive measures and publicized the incidents.

By doing so, it can be argued that Estonia opened itself up to potential embarrassment regarding the vulnerability of its cyber systems. However, Estonians indicate they vehemently wanted to demonstrate to the world what they believed to be a state-based attack from Russia. Moreover, they argue by being transparent regarding the 2007 events, it allowed both the internal business community and external partners (such as the United States, France, Latvia, Finland and NATO) to offer assistance in both short-term defensive capabilities and long-term defensive improvements (Estonian National Interviews 1-16 by Lochard 2016). Estonian cyber capabilities suffered blockages, but rebounded quickly. Their strong sense of pride toward their digital systems, along with momentum from the hybrid attacks, led to a long-term effort to strengthen national technical infrastructure.

3 SIMULATION MODEL

3.1 The Simulation Model

We built a simulation model based on the conceptual model described in section 2.2. The decision calculus in this model is formulated using the DYMATICA framework. DYMATICA is a system dynamics-based modeling framework created at Sandia National Laboratories for simulating systems that involve human behavior and decision making. The theoretical framework is based on well-established psychological, social, and economic theories that have been incorporated into a single structure (figure 2) that is both self-consistent and dynamic. Details can be found in Bernard et al. (2014) and Backus et al. (2010). DYMATICA uses a hybrid architecture with cognitive models implemented using system dynamics and embedded into an encompassing system dynamics model, which simulates interactions between people, groups, and physical, economic, or other system components.

The cognitive portion of DYMATICA begins with individuals or groups being exposed to cues (stimuli relevant to the decision maker). These cues are processed to create cognitive perceptions, the decision maker's assessment of the world or situation. Over time, cognitive perceptions become expectations, which are compared to cognitive perceptions to determine discordance with the current situation. Intentions are calculated using utility functions, and a multinomial logit function (McFadden 1982) compares intentions to determine behaviors, which over time become realized actions.

One of these cognitive models is populated for each individual or group being included in the model. The cognitive models are connected to each other and to a world model sector using system dynamics. The world model sector includes all of the non-cognitive components of the system of interest, including physical systems, economics, etc. In the Estonia model, the world model sector focuses on the physical characteristics of Estonia's cyber systems, including the strength of those systems, harm from cyber attacks, and effectiveness of cyber defense. This was simulated using typical system dynamics methodology, with cyber defense preventing a percentage of damage from the attacks, and the total damage causing a percentage drop in the health of the system. Outputs from the world model and the cognitive models act as inputs, or stimuli, for the cognitive models in subsequent time steps.

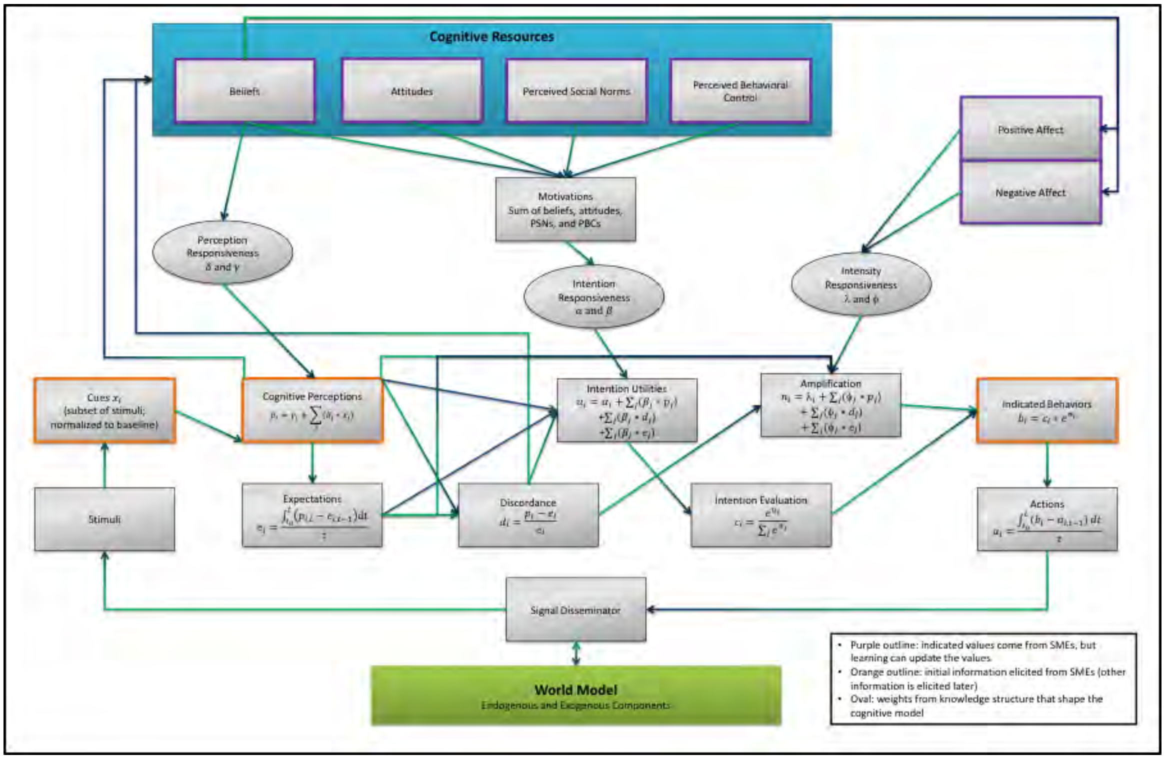
Cognitive Resources
Beliefs
Attitudes
Perceived Social Norms
Perceived Behavioral Control
Positive Affect
Negative Affect
Motivations
Sum of beliefs, attitudes, PSNs, and PBCs
Perception Responsiveness
δ and γ
Intention Responsiveness
α and β
Intensity Responsiveness
λ and ϕ
Cues x_i
(subset of stimuli; normalized to baseline)
Cognitive Perceptions
$p_i = \gamma_i + \sum_j (\delta_j * x_j)$
Intention Utilities
$u_i = \alpha_i + \sum_j(\beta_j * p_j)$
$+\sum_j(\beta_j * d_j)$
$+\sum_j(\beta_j * e_j)$
Amplification
$n_i = \lambda_i + \sum_j(\phi_j * p_j)$
$+\sum_j(\phi_j * d_j)$
$+\sum_j(\phi_j * e_j)$
Indicated Behaviors
$b_i = c_i * e^{n_i}$
Stimuli
Expectations
$e_j = \frac{\int_{t_0}^{t}(p_{i,t} - e_{i,t-1})dt}{\tau}$
Discordance
$d_i = \frac{p_i - e_i}{e_i}$
Intention Evaluation
$c_i = \frac{e^{u_i}}{\sum_j e^{u_j}}$
Actions
$a_i = \frac{\int_{t_0}^{t}(b_i - a_{i,t-1})\,dt}{\tau}$
Signal Disseminator
World Model
Endogenous and Exogenous Components
Purple outline: indicated values come from SMEs, but learning can update the values
Orange outline: initial information elicited from SMEs (other information is elicited later)
Oval: weights from knowledge structure that shape the cognitive model

Figure 2: DYMATICA computational structure.

3.2 Model Results

Initial results of the 2007 Estonian hybrid cyber attack model are shown below. These results are illustrative, and are likely to be updated upon further validation and consultation with subject matter experts. The results are meant to align with historical data on the 2007 riots and cyber incidents in Estonia, but are relatively course-grained and likely to look somewhat different than the data. For example, Estonia saw distinct waves of cyber attacks during the model’s time horizon, but the model smooths the incidents into a single wave.

Figure 3 shows model results related to rioting. The blue line shows the timeline over which Estonia moved the Bronze Soldier of Tallinn. This movement began on April 27, 2007, and was completed on April 30 of the same year. The attacker responds to a combination of warnings about moving the monument and the actual relocation by coordinating information campaigns, professional instigators, and riots in Estonia. These riots quickly materialize, as shown in green in figure 3. Rioting activity is caused by a combination of the coordination of riots by the attacker and initial discordance among that subset of the population about the move of the monument and bodies beneath it. The government uses law enforcement to try to control the rioting and decrease the potential for damage, as shown in gray. A separate subset of the population reacts to the riots and cyber attacks by counter-protesting (black line). Finally, in response to both the rioting and cyber incidents (discussed below), the United States, the European Union, and NATO denounce the events (brown line). This, along with the actual move of the Bronze Soldier of Tallinn and the bodies beneath it, and the push-back from ethnic Russians living in

Estonia who disapproved of the violence they witnessed in Tallinn brings the coordination of riots down to initial levels, tempering rioting and associated activities.

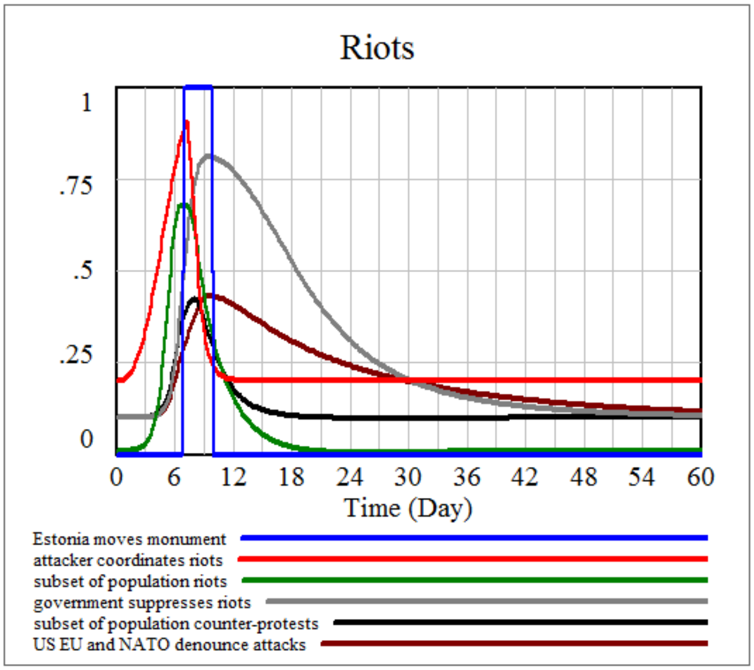

Figure 3: Model results regarding riots.

Figure 4 shows model results related to the cyber DDoS attacks. As with the rioting results, this scenario is spurred by the Estonian government moving the Bronze Soldier of Tallinn and bodies beneath it (blue line). This action causes the attacker to coordinate a series of cyber incidents against Estonia (red line). Cyber attacks (green line) increase relatively soon after the move of the statue and bodies beneath it and coordination of the attacks, and last for a few weeks, slowly decreasing by the end of the time horizon. Estonia quickly recognizes the DDoS attacks and accelerates its defense against them (gray line). Estonia chooses to publicize the attacks, requesting help from internal businesses and from allies. The United States, France, NATO, as well as Estonian businesses, assist Estonia with cyber defense (black line). The attacks cause the health of Estonia's cyber systems (brown line) to dip, but rapid and effective defense increases this health after a few days. Estonia uses the attacks to justify strengthening its cyber systems, and the health of those systems rises throughout the remainder of the time horizon.

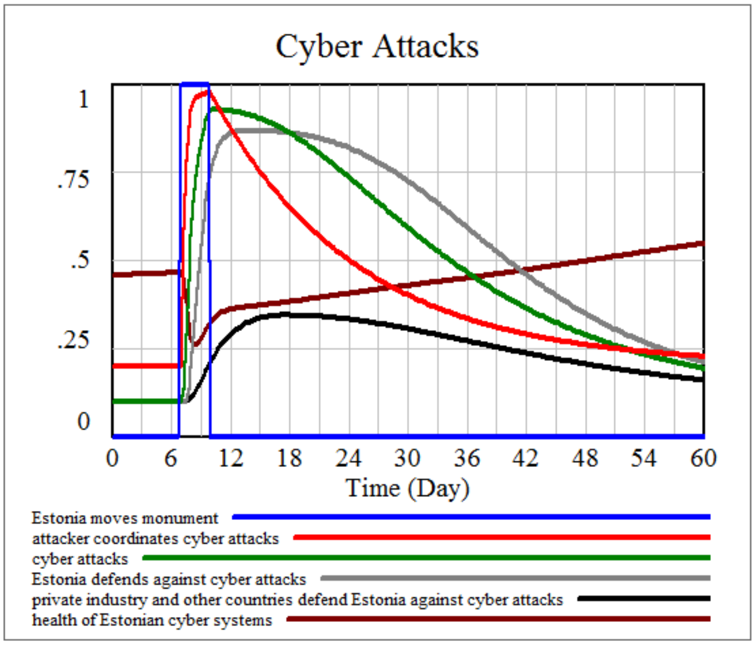

Figure 4: Model results regarding DDoS cyber attacks.

4 CONCLUSIONS

The 2007 DDoS attacks on Estonia proved that cyber incidents can be a major threat to modern society, and that cyber attacks might be combined with other actions, such as information operations and coordinated riots, to create further disruption. The potential susceptibility to cyber attacks and cyber warfare continues to grow as the world becomes increasingly dependent on such services. Concomitantly, cyber incidents by state actors have increased as these vulnerabilities have grown (U.S. Department of Defense 2015). Understanding a historical example of a major, politically-motivated cyber attack that was directed at a state and had significant impact can help us begin to understand the likely dynamics of such events, as well as potential responses and preparations that may make a system less vulnerable.

The model discussed here focuses on dynamics of the 2007 incidents in Estonia. It includes the information operations, rioting, and cyber attacks that emerged around the Estonian government's announcement it would move a Bronze Soldier of Tallinn and bodies beneath it, as well as the law enforcement and defensive responses that ultimately neutralized them. This model tracks historical events relatively well, which supports our causal hypothesis about the system's structure. To build this model we used the DYMATICA framework, which combines a carefully designed cognitive structure with system dynamics simulation. We worked closely with subject matter experts and employed field research and interviews to create the conceptual model as well as to design and populate the simulation model. We believe that combining this subject matter expertise with the DYMATICA framework provides a good foundation for understanding the causality behind the interactions and dynamics related to the 2007 Estonian attacks.

We hope that by understanding the causal structure of this historical experience we can gain insight into some of the fundamental reasons why the outcomes occurred as they did. In Estonia's case, short-term harm from these hybrid attacks led to long-term improvements and leadership in the cyber area. A deeper understanding of how to identify, prevent, and defend against these types of hybrid attacks in real-time is needed. We argue that utilizing the aftermath of such incidents to improve systems (rather than losing confidence and allowing degradation) is a potential major benefit of this type of model.

ACKNOWLEDGMENTS

We would like to acknowledge support for this work from the Office of Naval Research for its support on the "Behavioral Influence Assessment for Cyber Adversary Analysis" Project (Award NumberN0001415IP00069, Program Officer Dr. Rebecca Goolsby). Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly-owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Approved for unlimited release: SAND2016-3036 C. All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.

REFERENCES

Ashmore, W. C. 2009. "Impact of Alleged Russian Cyber Attacks." School of Advanced Military Studies, Fort Leavenworth, Kansas.

Backus, G., M. Bernard, S. Verzi, A. Bier, and M. Glickman. 2010. *Foundations to the Unified Psycho-cognitive Engine*. Sandia National Laboratories technical report, SAND Report 2010.

Estonian Nationals Interviews 1-16. Interview by Itamara Lochard. Personal interview. Tallinn, Estonia. February - June 2016.

McFadden, D. 1982. *Qualitative Response Models*. In Advances in Econometrics, Ed. Werner Hildenbrand, Cambridge University Press, New York.

Robinson, S., G. Arbez, L. G. Birta, A. Tolk, and G. Wagner. 2015. "Conceptual Modeling: Definition, Purpose and Benefits." In *Proceedings of the 2015 Winter Simulation Conference*, edited by L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, 2812-2826. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Statistics Estonia. 2015. "Statistical Yearbook of Estonia." Tallin, Estonia.

Tikk, E., K. Kaska, and L. Vihul. 2010. "International Cyber Incidents: Legal Considerations." Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia.

U.S. Department of Defense. April 2015. "The Department of Defense Cyber Strategy." Accessed March 2016. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

AUTHOR BIOGRAPHIES

ASMERET BIER NAUGLE is a researcher in the Cognitive Sciences and Systems Department at Sandia National Laboratories. She holds a PhD in Environmental Science from Washington State University. She is a system dynamics modeler with research interest in human behavior, model assessment, and creating hybrid simulation methods and strategies. Her email address is abier@sandia.gov.

MICHAEL L. BERNARD is researcher at Sandia National Laboratories. Michael holds a PhD in applied experimental psychology and is involved in the development of socio-cultural and geopolitical models of group/societal decision-making. Michael has contributed in the submission of over 80 articles and technical advance documents and reports in the field of human factors, general psychology, and group decision-making. His email address is: mlberna@sandia.gov.

ITAMARA LOCHARD is the Director of Cyber Policy Studies at George Mason University, Senior Research Fellow at the Center for Technology & National Security Studies at National Defense University, the Senior Researcher of International Security Studies at the Fletcher School of Law &

Diplomacy, and a certified mediator. She holds a PhD in international affairs, and presents on various aspects of irregular war and cyber/ICT issues at high-level government, NATO- and UN-fora. Her email is ilochard@c4i.gmu.edu.