Resilience of Critical Infrastructure Systems to Hybrid Threats with Information Disruption

Heimir Thorisson[1], Fabrizio Baiardi[2], David G. Angeler[3], Kuldar Taveter[4], Ashok Vasheasta[5], Paul D. Rowe[6], Wojciech Piotrowicz[7], Thomas L. Polmateer[1], James H. Lambert[1], Igor Linkov[8]

[1]University of Virginia, [2]Università di Pisa, [3]University of Nebraska – Lincoln, [4]Tallinn University of Technology, [5]International Clean Water Institute, [6]The MITRE Corporation, [7]Hanken School of Economics and University of Oxford, [8]US Army Corps of Engineers

Abstract

Technologies such as smartphones, identification, sensors, and actuators are the basic components of an infrastructure that offers efficiencies and conveniences for citizens, governments, and organizations. This infrastructure faces a variety of threats including kinetic assaults, natural hazards, and accidents as well as information disruption and misinformation. Furthermore, interdependencies among components increase the vulnerabilities of infrastructures. This chapter identifies challenges and solutions to countering hybrid threats by describing data availabilities and needs and by reviewing available theory and methods, even from other fields. The chapter reviews current and ongoing scenarios to assess forecasting methods for future one. Lastly, it also offers some guidelines to increase infrastructure resilience.

Introduction

Information technology has an increasingly large role in the day-to-day life of citizens in many parts of the world. Technologies such as smartphones, electronic identification, distributed controls, sensors and actuators, and others, often referred to as the Internet of Things (IoT), have promoted efficiencies and conveniences for citizens, governments, and organizations. National critical infrastructures face a variety of threats including kinetic assaults from adversaries and natural hazards and accidents as well as information disruption such as hacking of control or support systems, misinformation, and others. Furthermore, the reliance on information and communication technology and the connectedness of most critical infrastructures (electricity, communications, information, financial and government services, etc.) result in new vulnerabilities that can be exploited (Linkov et al., 2018). The European Centre of Excellence for

Countering Hybrid Threats characterizes *hybrid threats* as coordinated and synchronized actions targeting the vulnerabilities of states and organizations through various means, including but not limited to political, economic, military, and information (The European Centre of Excellence for Countering Hybrid Threats 2017). This chapter summarizes discussions and lessons learned from a working group at a NATO Advanced Research Workshop on Security and Resilience of Information Systems Affected by Hybrid Threats as it pertains to critical infrastructure, held in Pärnu, Estonia on 26-29 August, 2018.

Purpose and scope

A main challenge in effectively countering hybrid threats is to evaluate the resilience of systems in terms of "what," "why," and "who" of attacks. A characteristic of hybrid threats is that there may not be an agent claiming responsibility for an attack while no evidence for attributing the attack can be collected. The motivation and intention of the attacking agent may be several degrees removed from the location where a vulnerability is being exploited and attack detection can be time and resource consuming. Therefore, developing protocols to define the scope of attacks and identifying relevant agents is an important step towards predicting future targets and initiating countermeasures. The engagement of different levels of government is required and cross-organizational communication protocols should specifically address responses to hybrid threats.

The aim of this summary chapter is to identify challenges and solutions to countering hybrid threats in information and communication infrastructures. This includes documenting available theory and methods, including analogous methods from other fields, and describing data availabilities and needs. Lessons are derived from past and ongoing scenarios and incidents, and methods for forecasting emerging and future scenarios are reviewed. Recommendations for research and practice to increase the resilience of infrastructure are provided.

Background

This section identifies relevant literature on hybrid threats, classification of security threats, and modeling methods for information systems. Jouini et al. (2014) propose a classification model for security threats in information systems. They consider five criteria: source of threat, agents (human, environmental, technological), motivation, intention, and impacts. The impacts are further classified into different levels of destruction, corruption, or disclosure of information, theft or denial of service, elevation of privilege, or illegal usage. However, in a later publication (Jouini et al. 2016) the same authors note that this classification is limited, especially when it comes to hybrid threats. Due to the connectedness and strategic focus of hybrid threats, criteria may interact and threats may target multiple levels of a single criterion (a cyber attack coupled with misinformation). Understanding the connections and interactions of the different sources, agents, intentions, and threats, is therefore necessary to be resilient to a hybrid attack.

Thiele (2016) emphasizes the need for resilient systems to hybrid threats. Decision making across multiple sectors and hierarchies must be cross-linked to overcome the exploitation of diverse vulnerabilities. Thiele identifies four focus areas to enhance resilience: identification of key vulnerabilities, synchronization of cross-governmental decision making, military sustainability and civil preparedness, and balancing resource allocations. Schaub et al. (2017) discuss specific strategies to enhance resilience in the Baltic states: Estonia, Latvia, and Lithuania. These include increasing the independence of energy supplies and improving undersea and maritime communication and energy infrastructure. Furthermore, the resolution of maritime boundary disputes between Baltic region countries can eliminate a vulnerability that could be exploited by adversaries.

Mälksoo (2018) discusses emerging practices within NATO and the EU on countering hybrid threats. They note the recent emphasis within organizations on resilience as a critical institutional capability in the face of the deep uncertainty posed by hybrid threats. Resilience thus calls on individual member states and their populations and institutions to take responsibility, particularly in cyber security, rather than relying purely on conventional military defense.

Motus et al. (2018) propose a suite of interoperable modeling techniques with the aim of creating situational awareness in a system of systems. Together, the models describe the behavioral aspects of a cyber-physical system and can be used to explore the implications of hybrid threats to system behavior. The model suite puts emphasis on interdependencies of system components, data integrity, stakeholder interest and requirement modeling, and mental models. CyGraph is a tool introduced by Noel et al. (2016) for performing and visualizing graph analytics for situational awareness based on observed dependencies. Emerging technologies such as blockchain technologies are promising for managing data in intelligent distributed systems (Calvaresi et al.

2018; Trump et al., 2018). Automation of risk assessment in information systems has been proposed by Baiardi et al. (2016; 2015; 2014). They build a model of the information system and apply a Monte Carlo method to the simulation of attack chains on the various system components. In an iterative approach, countermeasures can then be implemented in the model and evaluated against the same attack scenarios by measuring the residual risk after applying countermeasures. In a similar vein, Musman et al. (2018) provide a method that quantitatively identifies risks to a system. They take a game-theoretic approach for determining the optimal allocation of resources to mitigations. Kholidy et al. (2016) focus on a cyber defense strategy for cloud computing, another increasingly prevalent technology.

Environmental science uses cumulative risk assessment to assess risk from aggregate exposure to multiple chemical, biological, or physical agents. Due to its emphasis on multiple threat agents and their interactions, cumulative risk assessment has potential to contribute to development of counter-measures against hybrid threats in critical infrastructure. MacDonell et al. (2018) characterize risks for cumulative risk assessment, noting that complexities of interactions between agents, often coupled with incomplete information, necessitate expert judgment and semi-quantitative methods for decision making. They identify three approaches to characterize the risks: making a multi-route hazard index, grouping stressors by exposure and toxicity, and screening indices for multiple factors and conditions. Backhaus et al. (2013) discuss the challenges of implementing cumulative risk assessment in European policy, including the collection and consolidation of empirical evidence. In infrastructure resilience to hybrid threats, there is a similar need for creating a body of knowledge of current and historical incidents and a characterization of their attributes.

Modeling of interdependencies of critical infrastructure has received considerable attention in the literature. Wu et al. (2016) include physical and geographic interdependencies to model cascading failures in an energy infrastructure system under terrorist attacks. Ouyang (2016) identifies vulnerabilities and critical locations in a power and gas system that is attacked at spatially defined nodes. Heracleous et al. (2017) provide an overview of several methods, including input-output models, agent-based modeling, and network models, in addition to proposing an approach using hybrid automata that combine discrete events and continuous time dynamics. The network model seems to be the most common approach and has been used to evaluate the impacts of attacks on critical infrastructure. Nan and Sansavini (2017) quantify the system resilience and introduce a hybrid modeling approach for decomposing the infrastructure network into components and defining their interactions.

Vaseashta et al. (2014) discuss a policy framework to enhance the critical infrastructure security of a nation through a systematic process, viz. to establish a national cyber risk governance model. This model defines risks and levels of risk tolerance under varying circumstances, assigns responsibility among various stakeholders for defining and managing assigned risks, sets risk management goals and metrics. It also determines conditions for evaluating and refining the model as circumstances warrant. Finally, it identifies and allocates resources to meet risk management; and codify appropriate policy-setting mechanisms, chosen from those that are constitutionally available. Possible mechanisms include national or regional legislation, executive order, and non-binding coordinating framework.

One primary dimension of the effectiveness of interventions to improve cyber resilience is that of scale. Solutions in the area of governance and policy typically have slow but large-scale effects on organizational structure and dynamics. In contrast, many technological interventions work at very fast speeds, but are necessarily limited to local effects. A comprehensive approach to ensuring information infrastructure is resilient to hybrid threats must adopt a portfolio of available interventions at many scales of operation. This is a consequence of what Bar-Yam (2004) has called the Multiscale Law of Requisite Variety (MLRV). Generalizing Ashby's Law of Requisite Variety in cybernetics (Ashby 1956), Bar-Yam suggests that environmental and adversarial effects and potential mitigating interventions have a natural scale at which they act. A system which lacks enough interventions at any scale cannot reliably be controlled. With his colleagues, Bar-Yam has since developed the foundations for a rigorous theory of multiscale information that can serve as a mathematical basis to support the MLRV (Allen et al. 2017). While this theory has yet to be applied to the analysis of cyber resiliency, it is a useful lens through which to view the varied pathways to resilience considered in the next section.

Pathways to resilience

Resilience of information infrastructure against hybrid threats should be increased through three interdependent pillars: technology, policy, and education (Linkov & Trump 2019). This section discusses several pathways to increase the resilience of information systems, summarized in Table 1, with an emphasis on scientific theory and methods that support each of the pillars.

Table 1. Theory and methods enhancing resilience of information systems to hybrid attacks, through technology, policy support, and interdisciplinary learning.

Type	Theory/methodology	Sample sources
Technology	Cryptographic analysis	Pike et al. (2006), Rowe et al. (2016)
	Vulnerability scanning	Holm (2011)
	Misuse and anomaly detection	Buczak and Guven (2016)
	Correlation	Baiardi (2018), Zhou (2010)
	Virtualization	Salapura (2018), Winarno (2015), Brendan (2008)
	Attacker simulation	Assante (2015), Baiardi (2016), Nicol (2004)
Policy support	Observe-Orient-Decide-Act principle	Heikkilä et al (2015), Rosquist et al (2017), Havlik et al (2015), Shvartsman et al (2010)
	Ontology alignment	Lister et al (2006)
	Cyber insurance	Romanosky et al. (2017), Pal et al. (2014)
Interdisciplinary learning	Complex adaptive systems	Angeler et al. (2018), Allen et al. (2014)

Technology

Cryptographic algorithms and protocols are often the strongest yet most fragile pieces of information infrastructure. Although leveraging mathematical weaknesses to cryptanalyze encrypted messages requires a large amount of time, a successful attack that steals the encryption key results in an irreversible compromise. It has been known for decades that the most widely used public key cryptographic algorithms would be vulnerable to key recovery attacks performed by a quantum computer. The most viable approach to defend against the possible development of quantum computation is to adopt and deploy “post quantum” algorithms that are resistant to quantum attack (Bernstein et al. 2009). Even in the absence of quantum computation cryptographic algorithms, computational attacks against crypto algorithms and protocols have been successful. Tools such as Cryptol (Pike et al. 2006), CryptoVerif (Blanchet 2007), and EasyCrypt (Barthe et al. 2013) leverage the mathematical rigor of formal methods to analyze the strength of cryptography against computational attacks.

Strong crypto, however, is not enough. Cryptographic protocols compose cryptographic primitives (such as encryption and hashing) in complex ways that sometime provide a network-based attacker the means to thwart authentication or confidentiality without breaking the underlying cryptographic algorithms. Symbolic cryptographic analysis tools such as CPSA (Ramsdell et al. 2009) or Maude NPA (Escobar et al. 2007) automatically discover the possibility of such network-based attacks against the logic of the protocol design. CPSA even allows the analyst to measure the relative strength of alternative protocol designs (Rowe 2016).

There is also a need to identify links between cryptographic resistance and system resilience. Hardening systems can make breaching the system more difficult for adversaries, but it can also complicate detection and response to breaches, thus possibly decreasing the resilience of a higher-level system. Standards and guidelines for information security have been developed, notably the ISO 27000 information security management system. However, several alternative standards have been proposed and this reveals the lack of a general consensus on which standards are appropriate in different industries and applications (Zhou et al. 2017). When updating cryptographic protocols, it should be estimated for how long they would be effective, or what their time to failure or obsolescence is. The social aspect, including when and where to realize data integrity, confidentiality, and accessibility, must be considered.

Some technologies have shown their potential to increase resilience. An example of these technologies is active vulnerability discovery, which includes both active and passive vulnerability scanning (Holm 2011). Active scanning introduces modules that interact with system nodes to build an inventory that lists the system nodes and the software components they are running. The output of this scanning updates an inventory of system components. By accessing databases that list public vulnerabilities for each component, the inventory of the components can be easily mapped onto a list of the system vulnerabilities. Passive scanning is a non-intrusive technology where the scanner only sniffs messages to discover the software components that produce the messages. This technology is less accurate than its active counterpart but it does not generate noise. Some integration of the two technologies results in an optimal compromise between accuracy and noise. Both active and passive scanning can discover changes in the number of physical nodes, in virtual machines, and in the interconnection topology.

Advances in data mining and machine learning have provided novel techniques to identify attacks targeting information systems. Buczak and Guven (2016) conducted a survey on machine learning and data mining methods for intrusion detection. They note three classes of methods in the surveyed literature: misuse-based methods detecting signatures of known attacks, anomaly-based methods in which anomalies in system behavior are flagged, and methods combining misuse-based and anomaly-based methods. They find that misuse-based methods require frequent updates of the databases which are collecting characteristics of known attacks, but have a low proportion of false positive detection. On the other hand, anomaly-based methods can detect previously unknown attack profiles (zero-day attacks) but generate more false positives. Methods combining the two are advantageous because they apply anomaly detection to populate the databases of the misuse-based portion of the method, possibly with human intervention in the learning phase.

An important step after attack detection is correlation (Zhou 2010, Baiardi 2018). Attack correlation enriches the analysis of the current intrusion by merging information on several attacks. It may consider attacker internet address, merging the attacks from an address together with other ones from the same address or the destination (attacked) service, or even the date and time. Attack correlation can support attack attribution as well as the prediction of the next attacks, and the final goal of the attacker.

Virtualization technology (Brendan 2008, Salapura 2018, Winarno 2015) implements a computing environment as a set of interconnected virtual machines and is a key technology for resilience, as it completely decouples the implementation of a programming environment from the underlying hardware resources. A virtual machine is a self-contained, autonomous programming environment with OS, applications, and servers. It can be easily replicated for redundancy. Each virtual machine is mapped onto a physical one and it can be migrated to a distinct physical node in a fully transparent way. Furthermore, a system can easily create a cheap backup of a machine at any time. The ability to store this backup on a distinct node is the basic mechanism for reconfiguring and recovering the service after an attack or a fault.

Virtual machine run time migration is also a defense mechanism as it obfuscates which physical node should be attacked to target a virtual machine. This supports active deception strategies that migrate each machine to a randomly selected node with a predefined frequency. This strongly increases the needed complexity of any attack on the virtual machine of interest.

The last technology of interest is attacker simulation. It can simulate both safety and security related events (Nicol 2004). The former includes faults, natural event, and involuntary errors by users or administrators. Security events are due to intelligent attackers that produce a sequence of attacks because a single attack does not allow the attacker to acquire the access rights which they seek. Hence, the attacker escalates their privileges by chaining attacks and using the privilege an individual attack returns to execute the following ones. The simulation can anticipate the chains of an attacker among those enabled by the system vulnerabilities. The simulation exploits information on the preferences and priorities of each attacker. Attacker simulation may adopt a Monte Carlo method (Baiardi 2016) if stochastic factors affect the output of the action by the attacker.

Attacker simulation assumes that some attackers are known and information on their strategies and preferences is available. As cybersecurity threats are extremely dynamic and unpredictable, an inventory of possible attackers should exist and be frequently reviewed and updated using information from threat intelligence. The attacker kill chain (Assante 2015) and MITRE ATT&CK^{TM} (Strom et al. 2018) are two methodologies for categorizing adversary activities that have been developed on the basis of threat intelligence. This more faithful view of adversarial capabilities supports full-scale emulation of the various steps of an attacker to reach their goals. CALDERA (Applebaum et al. 2016) is a red team emulation system that goes beyond exploitation of known vulnerabilities to automatically probe a system for weaknesses. It can provide a faithful understanding of how a target system reacts to adversarial attacks.

Policy support

Resilience manifests itself in the general population and workforces and education on responsible cyber conduct, recognizing the early warnings of a cyber attack, and defensive protocols during an attack should be given to individuals and organizations (Harrop and Matteson, 2015). The following considerations are important to model the resilience of critical infrastructures:

- Parameters for identifying "Who's in Charge?" and event classification such as whether the affected parties are private or public, what information is shared among the various stakeholders, and whether the level of response is from law enforcement, nation response, international response. This helps to define the legal construct required for governmental intervention or support of critical infrastructures.
- The evolution of the technology outpaces the ability of the judicial branch to create legislation that balances the operators of critical infrastructures with the societal responsibilities of essential services, continuity of government, and a safe and secure cyber infrastructure. The elements of this gap between legislation and technology begin to be identified and considerations for the legislative approach emerge.
- Identification of stakeholders is required to develop a cyber security policy, and understanding the inherent conflicts among them which can create natural tensions in policy. Building a model can help understand the nature of the problem and explore how stakeholders might interact during scenarios of various severities.

To manage hybrid threats with information disruption, stakeholder decisions need to be supported in the best way possible. Efficient decision-support can be arranged based on experience received from recent projects (Shvartsman, et al., 2010; Havlik, et al., 2015; Heikkilä, et al., 2015) and theories developed from that experience (Rosquist, et al., 2017) for supporting decision-makers by computer-based simulations and serious gaming. The iterations of simulations for decision-support are rooted in the OODA (Observe-Orient-Decide-Act) principle. In such simulations, information flows originating from different sources correspond to the Observe component; processing and analysis of the information correspond to the Orient component; decision-making corresponds to the Decide component; and executing simulations corresponds to the Act component. The results of the Act component provide feedback for the Orient and Decide components of subsequent iterations. A generic decision model can be worked out that connects three basic components in the response decision process: the stochastic information flow; situational awareness in establishing a spatiotemporal risk picture; and decisions to allocate resources for first response to the crisis under way. The generic decision model is based on the reference decision model put forward by Rosquist, et al. (2017), combined with the stochastic Marked Poisson Process (Snyder & Miller, 1991), and the theory of recognition-primed decisions (Klein, 1999).

Ontology alignment is another technique that can be applied to tackling information disruption (Lister et al, 2006). It helps to determine what the structure and meaning of information flows is based on data from other information source(s) of the same purpose.

Cyber insurance has emerged in recent years with policies covering liabilities for data breaches involving personal identification numbers, credit card and bank account information, and other sensitive personal information. It has been debated whether cyber insurance can in the long run enhance the security of a system (Pal et al. 2014); this depends on the economic behaviors of the insurers and the insured. Aspects of cyber insurance that diverge from traditional insurance practices are the extent of interdependent security and systematic risk among computer networks (Romanosky et al. 2017).

The resilience of a system is an emergent property arising from the kinds of responses its architecture allows. Resiliency should therefore be an important consideration in the design, engineering, and adoption of information infrastructure technologies. Given the wide variety of technologies and deployment environments, a systematic approach for addressing cyber resiliency in system design is valuable. Bodeau et al. (2011) have developed a comprehensive cyber resiliency engineering framework. Many of these ideas are being incorporated in official policy guidance published by the National Institute of Standards and Technology (NIST 2018). The scale at which this guidance applies is too large to prescribe particular solutions. This was an important consideration in the development of a higher-level set of resiliency design principles to help engineers navigate through the varied possibilities in the design space (Bodeau et al. 2017).

Informed decision-making by inclusion of knowledge base, analytical capability, foresight, and guidance plays a major role in futures-oriented analytical methodologies including heuristics, data mining, scientometrics, scenario development, and modelling and simulation to provide solutions and analyze their potential for integrated, novel and/or unconventional manifestations. Using a "framework by design" of emerging scientific and technological advances and trends, Vaseashta (2014) developed systematic and strategic methodologies and decision support tools to understand current, future, and varying challenges, as well as opportunities to create fully integrated solution pathways which include challenges to critical infrastructure.

Interdisciplinary learning

Significant strides forward have been made in our understanding of cyber security related issues. A conclusion that crystalizes from this chapter is that cyber security emerges from the complex interplay of a plethora of agents in a complex adaptive system (CAS). Complex adaptive systems are ubiquitous and occur, for instance in ecological, technological, and social systems. Central features of complex systems are hierarchical organization and the ability to exist in alternative system regimes (Holland 2014; Florin et al., 2018). These features influence – both individually and collectively – the resilience of complex systems. In this section we provide insight from other scientific disciplines, including psychiatry (Angeler et al. 2018) and social-ecological systems (Allen et al. 2014), to inform our understanding of cyber security with the help of advances made in resilience theory in other fields. Despite inherent differences between knowledge domains, distinctly different complex adaptive systems share several basic features, which allows for cross-fertilization and the potential development of an interdisciplinary approach to problem solving.

Several implications follow from the above-listed CAS characteristics:

1. *Hierarchical organization*: Rather than being scale invariant, complex systems are hierarchically structured, meaning that pattern-process relationships are compartmentalized by discrete scales of space and time. Imagine, for example, a lake: a microscopic organism exploits its habitat within a few milliliters of water and has very short generation times. In contrast, a predatory fish, such as pike, exploits the whole lake and has much longer generation times than the microorganism. Both organisms are unable to exploit the scale of the other. Considering scale in complex systems is important because disturbances are scale specific (Nash et al. 2014). For instance, a hail shower has a significantly higher impact on seedlings in a forest compared to on the trees. It follows that unaffected or least-impacted scales in a CAS can buffer against disturbances and maintain overall system functioning. Provided that cyber infrastructure is

hierarchically organized, this suggests that the identification of scalar relationships in these systems might offer opportunities to assess at which scale the systems are most vulnerable to attacks and how features of system structure and processes at other scales might mitigate the overall impact. Ecologists have developed statistical methods to discover scales in univariate and multivariate data (Angeler et al. 2016). These methods may potentially be valuable for assessing cyber risks.

2. *Alternative system regimes*: Complex systems are not infinitely able to cope with disturbances. Once a critical disturbance threshold is exceeded the system shifts from one configuration with specific pattern-process-feedback relationships to an alternative one with different sets of patterns, processes, and feedbacks (Holling 1973). Imagine a coral reef which shifts from a coral regime to an algae-dominated regime, or a healthy human subject who develops a chronic disease which is incurable. Both these regimes are stable, self-organizing, and self-perpetuating, which means that the algae regime will not return to a coral regime, nor the diseased person to a previous healthy condition. Several important implications for resilience follow that might inform cyber security. The reef example shows us that premises about complex systems are often reductionist and stationary, building on assumptions that the system is either robust or recovers to pre-disturbance conditions given enough time. In contrast, the consideration of alternative regimes accounts for the systemic complexity that emerges because of non-stationary conditions. The ability of CASs to recover *vs* undergoing a regime shift has led to the development of alternative resilience definitions that reflect these mechanistically distinct phenomena. Recovery, bounce-back or resiliency are all synonymous to engineering resilience and focus on single system equilibrium dynamics. In contrast, ecological resilience refers to a system's ability to change regimes and therefore accounts for non-linear dynamics, emergent phenomena and multiple equilibria (Angeler and Allen 2016).

Considering non-stationary behavior and distinguishing between resilience definitions is particularly relevant in times where humanity faces substantial and societal challenges, as cybersecurity issues illustrate, due to fast social-ecological change that pushes planet earth to a future without historical analogue. Information systems are developing so fast that it might not be optimal to facilitate recovery or adaptation within a potential system configuration that might be obsolete. For instance, rebuilding land line communication after a storm event seems unjustified in the face of future increases in the incidents and magnitudes of storms. Adopting such a management approach would only imply a costly and untenable coercion of the resilience of a system to maintain a ghost regime that is no longer viable.

Multiple equilibrium thinking, on the other hand, offers a gamut of potentially novel strategies to deal with the resilience of a cyber infrastructure in the future. Once strategies to foster the resilience of a desired cyber infrastructure regime fail, approaches can target the transformation of the system to a new, potentially more resilient regime (maybe at the expense of some performance figures). To this end, creative scenario planning that builds on transdisciplinary collaborations may assist in the design of systems that are resilient to a range of hybrid threats.

Interaction of cyber and physical systems

While cybersecurity cannot be neglected, it is also important that the digital dimension is interlinked with physical inputs and outputs. On the input side, cyber infrastructure relies on physical transmission, both wired and wireless, with other electronic equipment. This means that damage to physical elements of infrastructure influences the ability to operate the cyber infrastructure. On small scales, the problem is local, as transmission can easily be rerouted. However, when there is large-scale damage the recovery time is much longer, the same situation is in case of destruction of the key physical elements of the cyber infrastructure. Such physical threats exist despite increasing digitization. Moreover, telecommunication infrastructure could be interlinked with transport infrastructure (such as a fiber optics connection along a bridge), so damage of one element can cascade and result in damage to connected elements. A key danger is the reliance on electricity, as all elements of cyber infrastructure require energy. It is important to ensure that an alternative or emergency energy supply can sustain the operation of cyber infrastructure. This is especially important as electric networks can be relatively easily disturbed by physical attacks on the distribution system, or in the longer term, by disruption of fuel supply (coal, gas, etc.) for energy production. Such reliance is especially visible when looking at logistics and supply chain operations. Transportation systems processes increasingly rely on full, or partial, automation. As an example, container terminals at marine ports increasingly depend on automated handling equipment in addition to IT systems for managing processes. Modern handling equipment is designed for automated operations and there is no alternative option for manual operations. Failure of focal points of the transport system can in turn disturb whole production and retail networks that are based on Just in Time (JIT) principles. While cybersecurity is an important element, *hybrid threat* analysis must also consider the need for physical protection of critical assets and key staff.

Summary

As new technologies emerge, new threats follow in line. To build resilient information systems it is critical to think ahead and proactively address vulnerabilities that are exposed by emerging and future technologies, policies, and behaviors (Merad & Trump 2020). In the aftermath of the March 2018 Salisbury attack, the European Commission identified four areas where steps need to be taken to be better prepared for hybrid attacks: (i) situational awareness, (ii) strategic communication, (iii) building resilience and deterrence in cyber security, and (iv) building resilience to hostile intelligence activity (European Commission 2018). This summary chapter has identified theories and methods that echo these recommendations. This includes a proposed model for situational awareness in cyber-physical systems, emphasis on strategic communication across organizations, and techniques of cryptography, data mining, and machine learning to enhance cyber resilience in information systems. Future work should focus on the interactions between the different aspects of resilience and hybrid threats discussed. Accounting for the theoretical advances in other scientific fields may help operationalize challenges and help develop refined strategies for dealing with future hybrid threats.

Acknowledgments

The participants are grateful to colleagues who participated in the NATO ARW on Security and Resilience of Information Systems Affected by Hybrid Threats, held in Pärnu, Estonia on 26-29 August, 2018: Vladyslav Chevardin, Oleh Derevianko, Käsper Kivisoo, Indrek Künnapuu, Uko Valtenberg, and Besir Wrayet. The views expressed in this chapter are solely those of the authors, and do not necessarily reflect or represent the views of their affiliated organizations.

References

Allen, B.; Stacey, B.C.; Bar-Yam, Y. Multiscale Information Theory and the Marginal Utility of Information. *Entropy* 2017, *19*, 273.

Allen CR, Angeler DG, Garmestani AS, Gunderson LH, Holling CS (2014) Panarchy: theoryand applications. Ecosystems 17:578–589

Angeler, D.G**.** & Allen, C.R. (2016): Quantifying resilience. *Journal of Applied Ecology* 53(3): 617-624

Angeler, D.G., Allen, C.R., Barichievy, C., Eason, T., Garmestani, A.S., Graham, N.A.J., Granholm, D., Gunderson, L., Knutson, M., Nash, K.L., Nelson, R.J., Nyström, M., Spanbauer, T.E., Stow, C.A. & Sundstrom, S.M. (2016) Management applications of discontinuity theory. *Journal of Applied Ecology* 53(3): 688–698

Angeler, D. G., Allen, C. R., & Persson, M. L. (2018). Resilience concepts in psychiatry demonstrated with bipolar disorder. International journal of bipolar disorders, 6(1), 2.

Applebaum, Andy, Doug Miller, Blake Strom, Chris Korban, Ross Wolf: "Intelligent, automated red team emulation." ACSAC 2016: 363-373.

Ashby, W.R. 1956, An Introduction to Cybernetics, Chapman & Hall, 1956

Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*.

Backhaus, Thomas, Michael Faust, and Andreas Kortenkamp. 2013. "Cumulative Risk Assessment: A European Perspective on the State of the Art and the Necessary next Steps Forward." Integrated Environmental Assessment and Management 9 (4). Wiley-Blackwell: 547–48. doi:10.1002/ieam.1475.

Baiardi, F, F Tonelli, and L Isoni. 2016. "Application Vulnerabilities in Risk Assessment and Management." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 7 (2): 41–59. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84978376857&partnerID=40&md5=b4c072c500804a423815008f288f2853.

Baiardi, Fabrizio, Fabio Corò, Federico Tonelli, and Daniele Sgandurra. 2014. "Automating the Assessment of ICT Risk." *Journal of Information Security and Applications* 19 (3): 182–93. doi:10.1016/j.jisa.2014.04.002.

Baiardi, Fabrizio, Federico Tonelli, and Alessandro Bertolini. 2015. “Iterative Selection of Countermeasures for Intelligent Threat Agents.” *International Journal of Network Management* 25: 340–54. doi:10.1002/nem.

Bar-Yam, Yaneer. 2004. Multiscale variety in complex systems: Research Articles. Complex. 9, 4 (March 2004), 37-45.

Barthe, Gilles, François Dupressoir, Benjamin Grégoire, César Kunz, Benedikt Schmidt, Pierre-Yves Strub. “EasyCrypt: A Tutorial.” FOSAD 2013: 146-166.

Bernstein, Daniel J., Johannes Buchmann, Erik Dahmen, eds. *Post-Quantum Cryptography.* Springer Berlin Heidelberg, 2009.

Blanchet, Bruno. "A Computationally Sound Mechanized Prover for Security Protocols," in *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 193-207, 2007. doi:10.1109/TDSC.2007.1005

Bodeau, D., and R. Graubart, “Cyber Resiliency Engineering Framework (MTR 110237, PR 11-4436),” The MITRE Corporation, Bedford, MA, 2011.

Bodeau, D., and R. Graubart, “Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines (MTR 170001, PR 17-0103),” The MITRE Corporation, Bedford, MA, 2017.

C. Brendan, L. Geoffrey, et al, 2008,.Remus: High Availability via Asynchronous Virtual Machine Replication Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation , pp. 161-174

Buczak, A, and E Guven. 2016. “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.” *IEEE Communications Surveys & Tutorials* 18 (2): 1153–76. doi:10.1109/COMST.2015.2494502.

Calvaresi, Davide, Alevtina Dubovitskaya, Jean Paul Calbimonte, Kuldar Taveter, and Michael Schumacher. 2018. “Multi-Agent Systems and Blockchain: Results from a Systematic Literature Review.” In *Advances in Practical Applications of Agents and Multiagent Systems*, edited by Guillermo Vigueras, Juan M. Orduna, and Miguel Lozano, 110–26. Toledo, Spain:

Springer. doi:10.1007/978-3-642-12384-9.

D’Andreagiovanni, Michele, Fabrizio Baiardi, Jacobo Lipilini, Ruggieri Salvatore, Federico Tonelli 2018, “Sequential Pattern Mining for ICT Risk Assessment and Management”, *Journal of Logical and Algebraic Methods in Programming*, January 2019

Escobar, Santiago, Catherine A. Meadows, José Meseguer: “Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties.” FOSAD 2007: 1-50.

European Commission. 2018. “A Europe That Protects: EU Works to Build Resilience and Better Counter Hybrid Threats Brussels,.” *European Commission - Press Release*, June 13. http://europa.eu/rapid/press-release_IP-13-859_el.htm.

Harrop W., Matteson A. 2015. “Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA.” In: Lemieux F. (eds) Current and Emerging Trends in Cyber Operations. Palgrave Macmillan’s Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, London

Havlik, D., Deri, O., Rannat, K., Warum, M., Rafalowski, C., Taveter, K., Kutschera, P. & Meriste, M. 2015. Training Support for Crisis Managers with Elements of Serious Gaming. In: Denzer, R., Argent, R.M., Schimak, G., Hřebíček, J. (Ed.). *Environmental Software Systems. Infrastructures, Services and Applications* (217−225). Springer.

Heikkilä, A.-M., Havlik, D. & Schlobinski, S. 2015, Eds. Modelling crisis management for improved action and preparedness. *VTT Technology, 228*. Espoo, Finland: VTT Technical Research Centre of Finland Ltd.

Heracleous, Constantinos, Panayiotis Kolios, Christos G. Panayiotou, Georgios Ellinas, and Marios M. Polycarpou. 2017. “Hybrid Systems Modeling for Critical Infrastructures Interdependency Analysis.” Reliability Engineering and System Safety 165. Elsevier Ltd: 89–101. doi:10.1016/j.ress.2017.03.028.

Holland J.H. (2014) Complexity—a very short introduction. Oxford University Press, Oxford

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics*, *4*(1), 1-23.

Holm Hannes, Sommestad Teodor, Almroth Jonas, Persson Mats, (2011)"A quantitative evaluation of vulnerability scanning", Information Management & Computer Security, Vol. 19 Issue: 4, pp.231-247,

IRGC (2018). Guidelines for the Governance of Systemic Risks. Lausanne: International Risk Governance Center (IRGC).

Jouini, Mouna, and Latifa Ben Arfa Rabai. 2016. "A Scalable Threats Classification Model in Information Systems." In *Proceedings of the 9th International Conference on Security of Information and Networks - SIN '16*, 141–44. doi:10.1145/2947626.2947630.

Jouini, Mouna, Latifa Ben Arfa Rabai, and Anis Ben Aissa. 2014. "Classification of Security Threats in Information Systems." *Procedia Computer Science* 32. Elsevier Masson SAS: 489–96. doi:10.1016/j.procs.2014.05.452.

Kholidy, Hisham A., Abdelkarim Erradi, Sherif Abdelwahed, and Fabrizio Baiardi. 2016. "A Risk Mitigation Approach for Autonomous Cloud Intrusion Response System." *Computing* 98 (11). Springer Vienna: 1111–35. doi:10.1007/s00607-016-0495-8.

Klein, G. A. 1999. *Sources of power: How people make decisions*. Cambridge, MA: MIT Press.

Linkov, I., & Trump, B. D. (2019). The science and practice of resilience. Springer.

Linkov, I., Trump, B., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. Sustainability, 10(2), 440.

Lister, K., Sterling, L. & Taveter, K. 2006. Reconciling Ontological Differences by Assistant Agents. *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS-06): Future University, Hakodate, Japan, May 8-12, 2006.* Ed. Stone, P.; Weiss, G. ACM, 943−945.

MacDonell, Margaret M., Richard C. Hertzberg, Glenn E. Rice, J. Michael Wright, and Linda K. Teuschler. 2018. "Characterizing Risk for Cumulative Risk Assessments." Risk Analysis 38 (6). Wiley/Blackwell (10.1111): 1183–1201. doi:10.1111/risa.12933.

Mälksoo, Maria. 2018. "Countering Hybrid Warfare as Ontological Security Management: The

Emerging Practices of the EU and NATO." *European Security* 27 (3). Taylor & Francis: 374–92. doi:10.1080/09662839.2018.1497984.

Motus, Leo, Kuldar Taveter, and Veiko Dieves. 2018. "Modelling Complex System-Of-Systems for Creating Situation Awareness (Late Breaking Report)." In *2018 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, 168–70. Boston, MA: IEEE.

Nash, K.L, Allen, C.R., Angeler, D.G., Barichievy, C., Eason, T., Garmestani, A.S., Graham, N.A.J., Granholm, D., Knutson, M., Nelson, R.J., Nyström, M., Stow, C.A. & Sundstrom, S.M. (2014) Discontinuities, cross-scale patterns and the organization of ecosystems. *Ecology* 95(3): 654-667.

Nan, Cen, and Giovanni Sansavini. 2017. "A Quantitative Method for Assessing Resilience of Interdependent Infrastructures." Reliability Engineering and System Safety 157. Elsevier: 35–53. doi:10.1016/j.ress.2016.08.013.

National Institute of Standards and Technology, DRAFT Special Publication 800-160, Volume 2, *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*, March 2018.

Nicol D. M., Sanders W. H. and Trivedi K. S., 2004, "Model-based evaluation: from dependability to security," in *IEEE Transactions on Dependable and Secure Computing*, vol.1, no.1, pp. 48-65, Jan.-

S. Noel, E. Harley, K.H. Tam, M. Limiero, M. Share, CyGraph: Graph-Based Analytics and Visualization for Cybersecurity, Editor(s): Venkat N. Gudivada, Vijay V. Raghavan, Venu Govindaraju, C.R. Rao, Handbook of Statistics, Elsevier, Volume 35, 2016, Pages 117-167.

March.Ouyang, Min. 2016. "Critical Location Identification and Vulnerability Analysis of Interdependent Infrastructure Systems under Spatially Localized Attacks." Reliability Engineering and System Safety 154. Elsevier: 106–16. doi:10.1016/j.ress.2016.05.007.

Merad, M., & Trump, B.D. (2020). "Expertise Under Scrutiny: 21st Century Decision Making for Environmental Health and Safety. Springer International Publications. DOI: 10.1007/978-3-

030-20532-4

Musman, S., & Turner, A. (2018). “A game theoretic approach to cyber security risk management.” *The Journal of Defense Modeling and Simulation*, *15*(2), 127–146. doi:10.1177/1548512917699724

Pal, Ranjan, Leana Golubchik, Konstantinos Psounis, and Pan Hui. 2014. “Will Cyber-Insurance Improve Network Security? A Market Analysis.” In *IEEE Conference on Computer Communications*, 235–43. IEEE. doi:10.1109/INFOCOM.2014.6847944.

Pike, Lee, Mark Shields, John Matthews: A verifying core for a cryptographic language compiler. ACL2 2006: 1-10.

Ramsdell, John D. and Joshua D. Guttman. “CPSA: A cryptographic protocol shapes analyzer,” 2009. http://hackage. haskell.org/package/cpsa.

Romanosky, Sasha and Ablon, Lilian and Kuehn, Andreas and Jones, Therese. “Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?” (March 7, 2017). Available at SSRN: https://ssrn.com/abstract=2929137 or http://dx.doi.org/10.2139/ssrn.2929137

Rosquist, T., Havlik, D. & Meriste, M. 2017. A reference decision model of first responders' decision-making. *International Journal of Emergency Management, 13* (3), 193–209.

Rowe, P.D., Guttman, J.D. & Liskov, M.D. “Measuring protocol strength with security goals,” In *International Journal of Information Security,* 2016, volume 15, no. 6: pp. 575-596. doi:10.1007/s10207-016-0319-z

Salapura, V. and R. Harper, 2018, "Virtual Machine Resiliency Management System for the Cloud," in *IEEE Cloud Computing*, vol. 5, no. 3, pp. 55-64, May./Jun.. doi: 10.1109/MCC.2018.032591617

Schaub, Gary, Martin Murphy, and Frank G. Hoffman. 2017. “Hybrid Maritime Warfare Building Baltic Resilience.” *RUSI Journal* 162 (1). Routledge: 32–40. doi:10.1080/03071847.2017.1301631.

Shvartsman, I., Taveter, K., Parmak, M. & Meriste, M. 2010. Agent-Oriented Modelling for Simulation of Complex Environments. *The International Multiconference on Computer Science and Information Technology (IMCSIT 2010), Workshop on Agent Based Computing: from Model to Implementation VII (ABC:MI'10), Wisla, Poland, 18.10.-20.10.2010.* IEEE Computer Society, 209−216.

Snyder, D. L. & Miller, M. I. 1991. *Random point processes in time and space*. Springer.

Strom, Blake E., Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas. “MITRE ATT&CK^{TM}: Design and Philosophy (MTR 180360, PR 18-0944-11),” The MITRE Corporation, McLean, VA, 2018.

The European Centre of Excellence for Countering Hybrid Threats. 2017. “Hybrid Threats.” https://www.hybridcoe.fi/hybrid-threats/.

Thiele, Ralph D. 2016. “Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective.”

Trump, B. D., Florin, M. V., Matthews, H. S., Sicker, D., & Linkov, I. (2018). Governing the Use of Blockchain and Distributed Ledger Technologies: Not One-Size-Fits-All. IEEE Engineering Management Review, 46(3), 56-62.

Vaseashta, Ashok, Susmann, Philip, Braman, Eric. 2014. Cyber Security and Resiliency Policy Framework. Vol. 38 of NATO Science for Peace and Security Series - D: Information and Communication Security, IOS Press, The Netherlands.

Vaseashta, Ashok. 2014. "Advanced sciences convergence-based methods for surveillance of emerging trends in science, technology, and intelligence", Foresight, Volume 16 (1), pp.17-36, https://doi.org/10.1108/FS-10-2012-0074.

Winarno Idris, Ishida Yoshiteru, 2015, Simulating Resilient Server Using XEN Virtualization, Procedia Computer Science, Volume 60, Pages 1745-1752, ISSN 1877-0509,

Wu, Baichao, Aiping Tang, and Jie Wu. 2016. “Modeling Cascading Failures in Interdependent Infrastructures under Terrorist Attacks.” Reliability Engineering and System Safety 147. Elsevier: 1–8. doi:10.1016/j.ress.2015.10.019.

Zhou, Xiaojun, Zhen Xu, Liming Wang, and Kai Chen. 2017. “What Should We Do ? A Structured Review of SCADA System Cyber Security Standards.” In *Proceedings of 2017 4th International Conference on Control, Decision and Information Technologies*, 1–10. Barcelona, Spain: IEEE. doi:10.1109/CoDIT.2017.8102661.

Zhou, Chenfeng Vincent Leckie, Christopher and Karunasekera, Shanika 2010 A survey of coordinated attacks and collaborative intrusion detection, Computers & Security, Volume 29, Issue 1, Pages 124-140, ISSN 0167-4048.