Executive Masters in Cybersecurity
Brown University
Providence, R.I.

Adjuvant Security

A Cyber Legibility Primer

By

Michael T. Perrottet

27 February 2018

Brown Faculty Advisor: Timothy Edgar

Contents Page

Adjuvant Security

A Cyber Legibility Primer

This Page Is Intentionally Left Blank

Cyber Legibility Primer Statement of Intent

This Critical Challenge Project (CCP) addresses the lack of understanding inherent between private industry and the DoD and argues that not just a whole of government, but a whole of society approach is necessary for national security as it pertains to the cyber domain.

The desired end state of my CCP results in the development, publication, and promulgation of a cyber-legibility primer. Legibility refers to the state of understanding of an individual or group. Current operations in cyberspace are often either too technical or too fledgling to be universally understood, limiting their usefulness amongst state and non-state actors. This primer, or guide, is based upon the belief that enhanced cooperation between private and public industry provides mutual support and serves as an adjuvant to national security because it fosters understanding and facilitates decision-making.

The primer is written in six parts. Part I introduces the nature of cybersecurity and gives special recognition to previous work which was instrumental in the creation of the primer. Part II introduces several key characteristics including: comparative advantage, offense, defense, substrates, as well as the environmental characteristics of complexity, uncertainty, and ambiguity. Part III analyses four key principles of successful conduct within the operating environment. The four principles of leadership, cooperation, governance, and safeguards are followed by a breakdown of enablers in Part IV. Parts III and IV build upon existing international regime theory and offer up a new construct by synthesizing existing theory with proposed principles and enablers. V examines three key challenges which leave state and non-state actors vulnerable. The three challenges, cyber legibility, unity of effort, and planning are discussed in general throughout the paper, but are explored in detail in Part V. The paper concludes with recommendations in Part VI and distinguishes between recommendations pertaining to people, process and technology.

The cyber legibility primer will address capabilities within the various sectors as well as what limitations exist. The primer will analyze policy and technological constraints as well as legal restraints. The primer will be written at the unclassified level and although it is intended for a wide audience, it is specifically written for those with cybersecurity in mind. Finally, the ultimate goal of the cyber legibility primer is to enhance security through improved understanding and informed decision-making amongst private sector and government personnel.

This Page Is Intentionally Left Blank

Cyber Challenges and Adjuvants

Part I:
Introduction

The ubiquitous information environment requires a mental construct capable of addressing challenges to appropriate stakeholders. Existing constructs focus on technical characteristics such as network integrity, defensive, and offensive operations on the one hand and archetypal regimes to include realism, liberal institutionalism, and constructivism on the other. However, a holistic approach must lay more credence to effective cyber governance education, informed leadership, transparent public-private partnerships and lasting international cooperation.

The purpose of this paper is to improve mutual understanding and decision-making by establishing principles, identify enablers, and provide recommendations to existing mental constructs of the cyber domain in order to give stakeholders the ability to make better decisions in a complex, uncertain, and ambiguous environment. After examining several environmental conditions, the paper introduces four key principles: *Leadership, Cooperation, Governance, and Safeguarding.* These principles are enhanced by several enabling functions to include education, standardization, communication, stakeholder engagement, unity of effort and strategic context. While this list is not representative of all enablers, they are the most important. The paper highlights several challenges and concludes with a list of practical recommendations. Combined these principles, enablers, and recommendations enhance the current understanding of shared expectations about appropriate behavior, or norms.

Put another way, they enhance existing mental and physical constructs within the cyber domain by serving as an adjuvant to stakeholder decision-making. In medical terms, an adjuvant is a substance

that improves the effectiveness of a vaccine by "improving the body's response to a vaccination."[1] While an adjuvant substance does not improve the immune system itself, when used in conjunction with a vaccine, adjuvants ensure that the body develops enough antibodies to protect itself from the targeted germ.[2] In other words, adjuvants do not produce immunity, but they do trigger better results in vaccines administered to fight against foreign pathogens. Applying this concept to the cyber domain, the following principles, enablers, and recommendations serve as stimulants to augment established principles and will have an adjuvant effect on decision-making. These adjuvants enhance the existing regime complex. For the remainder of this paper, the Enhanced Regime Complex, or ERC, will be used to describe the adjuvant effects of principles, enablers, and recommendations on the current regime complex.

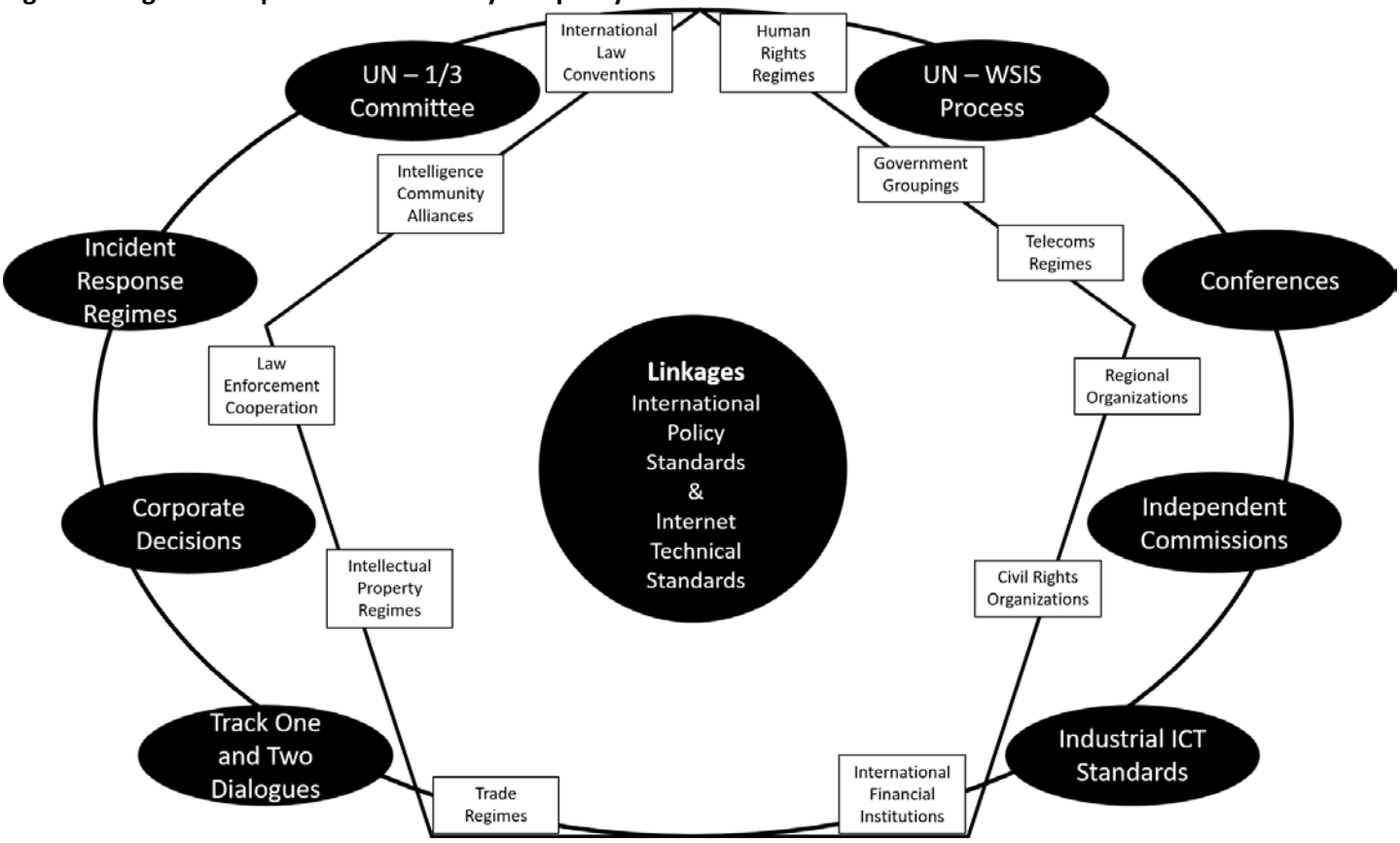
The paper is both informative and prescriptive, and like its predecessors, it does not assume to be complete. Indeed, the very nature of an adjuvant supposes that immunity cannot be achieved by itself. As such, these adjuvants draw upon existing policy, memoranda, orders, and directives with the express purpose of shaping future decision-making. It fulfills this task by providing stakeholders with the *means* to develop a statement of intent that guides decision-makers with the *ways* to implement informed decisions and establishes a framework for stakeholders to achieve mutually-beneficial *ends* irrespective of regime type.

Previous Work[3]

In 2014, Joseph Nye published a paper with the purpose of "mapping cyber governance using regime theory."[4] Beginning with Stephen Krashner's definition of regimes, that is those "principles, norms, rules and procedures that govern issue areas in international affairs,"[5] Nye outlines stakeholder interactions through various aspects of cyber governance to include standards, content control, and human rights[6] and identifies early on that insecurity results from the combination of low barriers of

entry as well as the fact that offense is cheaper than defense.[7] Recognizing the difficulty of having to protect the Internet for users to benefit from while also protecting users from what may come through the Internet, Nye examines advantages and disadvantages of differing regime constructs. Flexibility of the multi-stakeholder approach which stresses a collective approach to decision-making is contrasted against authoritarian regimes who's control over portions of the cyber domain serve as their primary characteristic.

Figure 1: Regime Complex as described by Joseph Nye*



**Sources: Image developed by Author. Content is from Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014), p8.*

Nye rejects the notion that any one regime theory (realism, liberal institutionalism, or constructivism), alone can best describe actions in cyberspace and concludes that the likelihood of single regime adoption worldwide for all cyberspace is low resulting from conflicting interests amongst

stakeholders.[8] Using the concept of a regime complex, or an informal and on occasion fragmented set of regimes, Nye, maps out a wide range of actors and activities (Figure 1). Separating the various layers of connectivity, his regime complex encourages a broad approach to understanding cyber governance in the global context. When mapping the Regime Complex as a whole, Nye is deliberately incomplete, in part because he recognizes the limitations of heuristic best practices.[9] Additionally, however, the environment he attempts to describe is extremely dynamic and he articulates four key dimensions of cyber issues: depth, breadth, fabric, and compliance (Figure 2). As they pertain to norms, depth refers to the "degree of coherence of a set of norms…breadth refers to scope of the number state and non-state actors that have accepted the norms…fabric refers to mix of state and non-state actors in an issue area…[and] compliance: how widespread is the behavioral adherence."[10]

Figure 2: Key Stakeholder Engagement Relative to Outcome Characteristics*^

Regime Construct	Key Stakeholder Engagement	Dimensions of Cyber Issues			
		Depth	Breadth	Fabric	Compliance
Linkage-Centric	Information Exchange Between Coalitions of Like-Minded States	High	High	Mixed	High
	Information Sharing Between Non-Like-Minded States	Medium	Medium	Tight	Mixed
Fragmentation-Centric	Balkanization	Medium	Low	Tight	Mixed
	Splinter-Net	Low	Low	Loose	Low

**Source: Developed by Author with the following additional references: "Depth," "Breadth," "Fabric," "Compliance," and Key Stakeholder Engagement Types are derived from Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014).*

^Note: Joseph Nye, describes topical issues using the four dimensions, however, the author of this paper has chosen to exchange cyber issues with key stakeholders, to demonstrate the utility of the four dimensions.

Part II:
Characteristics

1. Comparative Advantage: A Discussion on Offense and Defense

Operations in cyberspace are challenging the fundamental theory of war that a defensive position is stronger than an attack.[11] Increasingly, cybercriminals, state sponsored hackers, and other malicious actors find ways to circumvent or defeat defensive measures designed to keep them out. While the cost to the attacker is low, the damage sustained by an organization is disproportionately higher, often extending beyond the walls of the organization itself. Critical analysis reveals, however, that successful offensive attacks in cyberspace are made possible by ineffective leadership and poor management of cyber security assets within organizations that are attacked. This reinforces the notion that warfare has not changed. A defensive position can still be more advantageous than an offensive one regardless of the domain in which attacks occur. In cyberspace, however, attackers can gain a comparative advantage over defenders from better use of people, processes, and technology.

In the physical world, the advantages of a defensive posture are best described in Carl von Clausewitz's book, *On War*. A nineteenth century military theorist, Clausewitz defined the defense as a slow and methodical[12] period of waiting[13] intended to preserve forces[14] with the goal of returning to the offense.[15] He argues that defense is the stronger position because the passive act of waiting, as a function of preservation, is less costly and easier to conduct than the active purpose of the offense: victory.[16]

Strengths demonstrating Clausewitz's theory have occurred throughout history. For example, during the Peloponnesian War, Syracusan forces in defense of their city-state had intimate knowledge of key terrain, which the attacking Athenian lacked. The Athenians fought in unknown terrain that often resulted in the delivery of imperfect information, the dispersion of forces, and vulnerability to discovery and counterattack.[17] In contrast, the defense enabled Syracusans to leverage their knowledge of the local terrain to build effective walls, patiently wait, and plan counterattacks. Although, defense of the city restricted the Syracusan's freedom of movement, their posture supported interior lines of communication.

Operations in cyberspace achieve greater speed, scale, and surprise than are possible in the physical world. The Athenians' attack on Syracuse took months and ended in defeat, while attacks in cyberspace often occur faster than they are even detected. Further complicating the problem is that the scale of an attack does not necessarily increase detection rates and range from large data breaches on a single server to multiple smaller breaches that can add up over time. In 2011, for example, Visa estimated that small credit card data breaches accounted for 95 percent of their total credit card breaches.[18]

The increasing number of successful cyberattacks that go undetected lays credence to the argument that offense is the stronger posture in cyberspace. Despite these successful attacks, however, none demonstrate that offense is the stronger position because while speed, scale, and surprise affect offensive operations, they have a similar impact on defensive operations. Successful offensive operations derive a comparative advantage over defenders from their better use of people, process, and technology.

Historically, advantages in the offense have included surprise, movement, and the ability to maneuver forces around defenses as necessary. Conversely, advantages in the defense included better knowledge of terrain and more robust means of communication. Such distinctions no longer apply to

attacks in cyberspace, however, since the same potential advantages are available to both sides to achieve victory. What does exist is a *comparative advantage* of attackers in the offense. Clausewitz stated that comparative advantage exists when an attack is costlier for one side than the other.[19] In cyberspace, the offense maintains a comparative advantage over the defense in three areas: people, process, and technology.

People

First, people can provide a comparative advantage in offensive cyberspace operations if they achieve more effective collaboration and use of talent than the frequently poor leadership and human error in the defense. As a result, offensive attacks are often more successful because the attackers are more organized than the entity being attacked.

Warwick Ashford of *Computer Weekly* points out that in many instances, attackers collaborate with one another more effectively than the organizations being attacked and suggests that organizations must avoid the urge to assign all aspects of cyber security to an individual.[20] Instead, Ashford argues that effective cybersecurity requires more collaboration at all levels.[21] Moreover, collaboration must be expansive. Simple partnerships between similar organizations are insufficient. In 2015, for example, the U.S. Treasury department conducted an exercise known as the Hamilton Series. Financial experts discovered that a previously developed "buddy bank" system, in which two local branches agree to assist each other's customers in a crisis, failed to prevent the erosion of consumer confidence.[22] Effective alliances must ensure mutual and harmonious support, a concept that attackers have so far exploited better. In many instances, offensive actions owe their success to governments that endorse attacker efforts such as the Russian espionage group known as "Fancy Bear." Alternatively, governments conduct attacks without the use of proxy groups, as was the case when North Korea hacked Sony Pictures Entertainment in retaliation for the release of the film *The Interview*.[23]

Acquiring the best talent is another concern. Robert Hannigan, a former head of the United Kingdom's security and intelligence organization known as the Government Communications Headquarters, argues current cyber security hiring practices fall short for three reasons: age, gender, and cost. Identification of talent, Hannigan states is unsustainable if consideration only goes to males in their twenties, adding that hiring practices will be unsustainable if the primary method for hiring is to poach talent from other organizations using increasingly larger salaries.[24] The consensus of cyber security planning suggests hiring should focus on quality rather than scale. In 2012, the Federal Communications Commission (FCC) produced a *Cyber Security Planning Guide,* which outlines a hiring process designed to properly vet potential candidates to preserve the quality of employees.[25]

While collaboration and talent acquisition serve as force multipliers for offensive cyber-attacks, human error and poor leadership negatively impact defensive measures. As stated in the Harvard Kennedy School's *Cybersecurity Campaign Playbook*, human error facilitates most successful cyber-attacks.[26] The majority of human error is preventable and results from either ignorance or neglect, rather than the notion that the offense is inherently stronger than the defense. To mitigate human error, the *Cybersecurity Campaign Playbook* provides a simple list of the top five actions necessary for effective cyber security: setting the tone; use of two-factor authentication; use of strong passwords; ensuring a continuous and iterative approach to planning; and backing-up an organization's data and preparation. The first four are nearly free. The fifth recommendation, use of the cloud to backup and store data is relatively low cost when compared to what might result in the event of a successful attack.[27] In many high profile cyberattacks, such as 2017's Equifax data breach, organizations employed one-off defensive measures and did little to ensure proper updates were maintained.[28]

The most important human factor shortfall in the defense has been poor leadership. The ability to inculcate security into the organization's culture begins with the leadership's ability to foster a climate in which information security plays a leading role. Leaders must set the example by providing

clear guidance and assuming a visible role. Many existing organizations mistake management for leadership. Instead, organizations must think in terms of leading people and managing things. Additionally, the FCC's *Cyber Security Planning Guide* suggests that leadership and collaboration go hand in hand and calls for business leadership to work alongside technical expertise when developing defensive strategies.[29]

Process

The second potential comparative advantage of the offense over the defense in cyberspace has resulted from insufficient processes. For preservation to occur, a defensive process or framework must be guided by strategy. The National Institute of Standards and Technology (NIST) suggests a sound cybersecurity process can be achieved by incorporating five steps: identify critical functions and risk that are consistent with an organization's strategy; protect an organization by implementing safeguards; develop effective detection methods; ensure response is proportional to the threat; and finally, develop an appropriate recovery plan to ensure organizational resilience.[30] Unfortunately, many organizations fail to adhere to these recommendations. In the Equifax breach, the company failed to patch known vulnerabilities in a timely manner and while much of this resulted from poor leadership, the neglect could have been avoided by adherence to an established cybersecurity framework.

In most instances, however, laws restrict defensive cyber operations whereas most cyberattacks are conducted outside legal constraints. For example, financial services companies must meet payment card industry compliance requirements and healthcare organizations must comply with Health Insurance Portability and Accountability Act guidelines.[31] While some defensive postures prove effective, they are too often the result of autocratic state involvement. For example, the Chinese Communist Party fosters "social credit" by collaborating with app developers to provide mobile-based

services such as mobile bank pay. While these services are designed for convenience, they also track users and impinge on privacy.[32]

Still, defensive measures that focus only on prevention are insufficient. True mitigation requires an organization to transition out of the defense. Clausewitz called this transition "the flashing sword of vengeance,"[33] whereby a defense transitions to offensive operations. The concept of transitioning out of the defense is a critical component to Clausewitz's argument, first because it emphasizes the interrelationship between offense and defense to achieve victory. Second, transition is important because it demonstrates that objectives cannot be achieved through a defensive strategy alone.[34]

Short of government institutions, however, legal constraints prohibit most organizations from conducting offensive operations. Peter Cooper draws from military tactics to suggest in the *Journal of Law and Cyber Warfare*, that private organizations can conduct what the Department of Defense calls 'active defense.'[35] Active defense is the use of specific means to counter enemy actions in a specific area.[36] What defenders can do, Cooper argues, is be proactive and predetermine where the enemy is likely to attack next. Short of transition, organizations must better plan for continuity and ensure that a viable continuity of operations plan, or COOP, exists and is trained to.

Technology

Finally, the third comparative advantage that the offense has enjoyed is technology. Comparative advantage results from better integration of technology with elements of people and process to achieve objectives. By integrating technology into a larger strategy to include people and process, adversaries in the offense can exploit both human and technical vulnerabilities. In doing so, the defense is forced to address offensive attacks that are not only difficult to prevent, but are also increasingly complex, which makes them more difficult to understand.[37] For example, Magnus Revang of Gartner, an American research and advisory firm specializing in information technology, suggests that

while offensive deception attacks like fake news are conducted using artificial intelligence (AI), they are also the result of training people to develop more believable fake news.[38]

In contrast, poor defensive operations exist when a defensive strategy is based entirely upon a specific technology. Both NIST and Harvard's *Cybersecurity Campaign Playbook* acknowledge this tendency and write cyber security frameworks to ensure that specific technologies are integrated with both people and process. Michael Handel, a former professor of U.S. naval strategy at the U.S. Naval War College uses the term 'tacticization of strategy'[39] to describe the tendency of an organization to regard a low-cost system or weapon as a strategy rather than viewing it as a component limited to a specific task. When a defensive strategy uses technology, but is absent people and process, all that is required of the offense is a more advanced technology to overcome it. Sharon Thiruchelvam of *Raconteur*, argues that an arms race results since, according to Gartner, by 2020 AI will be sophisticated enough to create fake news reports more quickly than defensive AI's ability to detect and defeat them.[40]

The analogy of an arms race highlights the danger of a defensive strategy based upon technology alone. As a military strategist, Mao Tse-Tung warned against the overreliance of technology in warfare and stated, "the so-called theory that 'weapons' decide everything, which constitutes a mechanical approach to the question of war and a subjective and one-sided view…weapons are an important factor in war, but not the decisive factor; it is people, not things that are decisive."[41]

Instead, special training is required in the parts of organizations most likely to serve as the first line of defense against attacks. With fake news, for example, an active defense includes training helpdesk personnel to ensure that the source of inbound material has been authenticated.[42]

Counterargument

Some may argue that the offense is naturally the stronger position in cyberspace because, in contrast to kinetic conflict where signs of a possible attack become visible beforehand, this may not

occur in cyberspace. This suggests that the effectiveness of defensive measures is directly proportional to the degree of visibility of an attack. This logic assumes that inductive and deductive reasoning are both prerequisites to a successful defense.

In the past, the defense was easier because it was typically known who your enemies were, resulting in a certain kind of decision-making process. If the enemy was known, preparation of a defensive position allowed for deductive reasoning. General rules could be developed resulting in specific known conclusions. When deductive reasoning alone was insufficient, defenders could take specific observations to draw general conclusions, referred to as inductive reasoning.

In cyberspace, however, attribution is the Achilles heel of cybersecurity. Determining who the enemy is proves extremely difficult because of an increased ability to use deception and disguise. Absent an understanding of who the enemy is, it becomes impossible to develop a tailored defense based upon known conclusions about the enemy as is the case when employing deductive and inductive reasoning. Using the Sony hack as an example, in the backdrop of heightened tensions between the United States and North Korea, Sony lacked effective reasoning tools, which led to an ill-prepared defense against North Korean retaliation is response to the film, *The Interview*.[43]

While the degree of visibility to a pending attack is more difficult, the development of effective defensive measures does not require deductive and inductive reasoning alone. Louis Pasteur, a French microbiologist and inventor of the process of Pasteurization, once noted that "where observation is concerned, chance only favors the prepared mind."[44] Pasteur understood, that brilliant insights require preparation. Similarly, organizations today must plan for defense in cyberspace with a "prepared mind". A function of the prepared mind is *abductive* reasoning, which uses incomplete observations to make a best prediction or guess about what the enemy would do. Abductive reasoning is best for countering deception attempts since it is more expansive and considers as many outcomes as possible.

Comparative Advantage Outlook

Although attackers have maintained a comparative advantage over defenders in cyberspace resulting from the better use of people, process, and technology during an attack, a defensive position can be more advantageous than an offensive one regardless of the domain in which the attack occurs. For now, the attack is more advantageous because the concept of defense has been disorganized and incomplete and defenders have not yet grasped that comparative advantage can be negated by whomever is more organized and more collaborative. While former hacker Kevin Mitnick argues that "only amateurs attack machines; professionals target people," [45] this is only partially correct. Active defense requires the simultaneous use of people, process, and technology. Similarly, Clausewitz stated that various forms of defense are dependent upon factors such as fortresses, the people, and alliances,[46] but effective defenses require active management (active defense) as well as the prepared mind of leadership, without which capabilities could emerge as critical vulnerabilities.

2. Cyberspace Substrate[47]

One peculiarity pertaining to cyber domain is in the name itself. A 'domain' is by nature restrictive and the word literally confines mental constructs. The term 'domain' is administratively convenient, particularly for government organizations. For example, the Joint Publication 3-12 on Cyberspace Operations does not distinguish between the cyber domain and cyberspace stating that cyberspace is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space."[48] Scholars such as Daniel Kuehl align cyberspace and cyber domain even more bluntly stating cyberspace is "an operational domain framed by use of electronics to…exploit information via interconnected systems and their associated infra structure."[49]

Foremost, cyberspace is a substrate not a domain. A substrate is a material upon which others act. To conceptualize this, consider for a moment an enzyme growing inside a laboratory petri dish. It grows up and out and given enough time, can extend beyond the walls of the dish. In a sense, cyberspace constitutes a digital petri dish in which others act. While the concept of domain is restrictive, the key characteristic of a substrate is pervasiveness. But, while the substrate is by nature more pervasive, using current mental constructs the cyber domain is more holistic because it includes additional layers beyond simply the logical layers of the cyberspace substrate. Physical aspects of the cyber domain include geographic location and hardware such as undersea cables. Organizational aspects are also included, such as government policy, law, and supervisory layers. The physical, organizational, and logical aspects comprise the cyber domain, of which the cyberspace substrate is simply a part.

Some may argue that the distinction between cyberspace and cyber domain is irrelevant because the cyber domain encompasses additional aspects that the cyber substrate does not. Understandably, the benefits to aligning cyberspace with existing domains streamlines decision-making. The importance of the distinction, however, is that a substrate has characteristics that a domain does not. First, factors such as attribution, speed, scale, and precision apply to the cyber substrate, but not the cyber domain. Second, unlike a domain, whose operations often lead to capability partitioning (e.g. the Air Force, with the air and space domains; the Navy with the sea domain), the pervasive nature of the cyber substrate requires a measure of understanding with all domains beyond what is necessary between other domains.

What results is a required change to existing cyberspace mental constructs. Rather than thinking of the substrate in just logical terms, cyberspace should be considered across all aspects of regimes. Doing so facilitates, stakeholder engagement across multiple disciplines, which prevents the stove-piping of ideas and information.

Figure 3: Cyber Domain Relative to the Cyberspace Substrate

<table>
<tr><td rowspan="14">Cyber Domain Cyber – Key Terrain (C-KT)</td><td colspan="2" rowspan="3">Organizational</td><td colspan="5">Government Layer | Gov. Policies | Gov. Procedures | Nat'l/Int'l Standards | Law | Regulations| Agreements | Treaties</td><td>Government Security</td></tr>
<tr><td colspan="5">Organization Layer | Org. Policies | Org. Procedures | Org. Info Sharing Agreements</td><td>Organizational Security</td></tr>
<tr><td colspan="5">People-Supervisory Layer | CISO | CIO | CEO | Boards</td><td>Personal Security</td></tr>
<tr><td rowspan="10">Cyberspace Substrate</td><td rowspan="9">Logical</td><td colspan="5">Persona Layer | User IDs | Emails | Phone #'s</td><td>Identification and Authentication</td></tr>
<tr><td colspan="5">Software Application Layer | Web Browsers | Office Products</td><td>Application Security</td></tr>
<tr><td colspan="5">Operating System Layer | Windows | Android | iOS</td><td rowspan="5">Host Security</td></tr>
<tr><td colspan="5">Machine Language Layer | 01001110100111010111011010</td></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">Application</td><td rowspan="3">Data Messages or Streams</td><td rowspan="3">Telnet | HTTP | SMTP | FTP | TFTP | SNMP | DNS | DHCP | SSH</td></tr>
<tr><td>6</td><td>Presentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>Transport / Host-Host</td><td>Segments or Datagrams</td><td>TCP | UDP</td><td rowspan="2">Network Security</td></tr>
<tr><td>3</td><td>Network</td><td>Internet</td><td>Packets</td><td>BGP</td></tr>
<tr><td>2</td><td>Data Link</td><td rowspan="2">Network Access</td><td rowspan="2">Frames</td><td>IP | ICMP| ARP | RARP</td><td rowspan="2">Infrastructure Security</td></tr>
<tr><td colspan="2" rowspan="3">Physical</td><td>1</td><td>Physical</td><td colspan="3">Hardware | Cables</td></tr>
<tr><td>0</td><td>Geographic</td><td colspan="3">Geolocation and Dependencies</td><td>Physical Security</td></tr>
<tr><td>Layer</td><td>OSI</td><td>Internet</td><td>Data Format</td><td>Protocols</td><td>Security Type</td></tr>
</table>

(Source: Author).

3. Complexity, Uncertainty, and Ambiguity

Three key characteristics of the cyber substrate inhibit the ability to establish order across regimes of any type. Complexity, uncertainty, and ambiguity. Complexity refers to the manner in which aspects of the ERC are interdependent. Uncertainty is the state of awareness where the state of something within the ERC is unknown. Uncertainty can pertain to the type of consequences, the likelihood of occurrence (often expressed in terms of probability), the severity of the consequences, and the location of, or the time during which these consequences may occur.[50] Ambiguity refers to the

quality of being open to different interpretations resulting in unique perspectives and/or divergent actions between ERC stakeholders.

All three characteristics influence the decision-making environment. Depending on the type of actor, however, these characteristics can shape decisions in very distinct ways. For example, though uncertainty in industry often stems from free-market economic forces, it generally assumes stability in the larger socio-political-economic framework. Some government organizations such as the military, however, assume instability in the larger framework because the much broader range of threats, from humanitarian assistance to the existential nuclear threat. This leads to distinct forms of decision-making processes as a result.

Lucas Kello, in his book *The Virtual Weapon and International Order*, further describes the difficulties in developing a mental construct stating, [t]he growth of technological ability is rapidly outpacing the design of concepts to interpret it."[51] Perversely new technologies in cyberspace have democratized complexity, uncertainty, and ambiguity, resulting from adversaries operating across the cyber substrate with mass, speed, and precision once thought unimaginable. Because instability in the larger socio-political-economic framework must now be considered across the ERC, so too must several principles.

Part III:
Principles

The following four key principles of leadership, cooperation, governance, and safeguards address the complex, uncertain, and ambiguous environment of the regime complex as described by Joseph Nye. Throughout, enablers provide linkages used to interconnect the four principles across the ERC to include: standardization, communication, stakeholder engagement, unity of effort and strategic context.

Leadership

Operations in cyberspace are challenging a fundamental theory of war which states that a defensive position is the stronger form of war in contrast to an offensive attack.[52] Increasingly, cybercriminals, state sponsored hackers, and other malicious actors find ways to circumvent or defeat defensive measures designed to keep them out. While the cost to the attacker is low, the damage sustained by an organization is disproportionately higher, often extending beyond the walls of the organization itself. Critical analysis reveals, however, that successful offensive attacks in cyberspace are more a product of ineffective leadership within organizations that are attacked and similarly poor management of their cyber security assets, reinforcing the notion that warfare has not changed. In fact, a defensive position is more advantageous than an offensive one regardless of the domain in which attacks occur. In cyberspace, however, attackers have maintained a comparative advantage over defenders from their better use of people, process, and technology.

As stated in the 2015 National Security Strategy, "any successful strategy to ensure the safety of the American people and advance our national security interests must begin with an undeniable truth – America must lead."[53] Leadership serves as a force multiplier. Effective leadership establishes a unity of effort to promote innovation and enable the remaining three principles. Informed leadership when working in conjunction with additional ERC stakeholders, can provide strategic context. Strategic context is important because it helps to frame the problems in the context of the overall ERC environment.

Specific leadership challenges pertaining to cybersecurity include an overly complex command and control structure. Additionally, leaders who make decisions on cybersecurity often lack access to highly skilled and informed stakeholders with experience in cyberspace. The core framework for cybersecurity that is still developing will have effects on the ERC long into the future resulting in the need for leaders to ensure stakeholder engagement across multiple disciplines.

Cooperation

In the cybersecurity field, cooperation is often based on information sharing. Information sharing is the first core capability listed in Executive Order 13636, signed on February 12, 2013.[54] Information sharing as a function of cooperation is important, but the notion of sharing can be ambiguous. Information can be shared one way. Cooperation, though, is two-way and requires a certain degree of exchange. Information *exchange* establishes reciprocity that information sharing does not.

Cooperation through information exchange in cybersecurity is often difficult, however, because the parties considering information exchange either lack initial trust in each other or are bound by law to restrict access to certain information. The over-classification of information is often the principle challenge to information exchange and limits the potential for successful cooperation. Declassification

of threat indicators is universally beneficial and would facilitate resilience. Information exchange does not require total declassification of files. Methods such as the use of portion markers, which parse specific information for the purposes of sharing unclassified information contained within classified briefs is one tool but is time consuming and can be costly. An alternative, the Enhanced Cybersecurity Services (ECS) program, is designed to share classified information with infrastructure operators.[55] It serves as a useful tool, but the information is only accessible to those who already have clearance.

Even more important than the need for access to available information is the need for interdisciplinary discussions.[56] Lucas Kello of Oxford University, argues that not only is information exchange crucial, but the creation of new ideas must occur through a "concert of disciplines"[57] resulting from the need to address the increasing complexity, uncertainty and ambiguity of challenges. Meaningful partnerships can provide strategic peripheral vision and should be comprised of private industry, government, and military professionals with stated goals of improving universal understanding of cyber-related challenges, eliminating ambiguity, expediting the flow of information, and improving resilience in areas pertaining to critical infrastructure.

Analysis of the different forms of cooperation elsewhere, however, demonstrate that current sharing amongst ERC stakeholders is insufficiently leveraged. The National Institute for Standards and Technology (NIST), for example, is a key stakeholder in the ERC and provides several useful toolkits for government and non-government organizations alike. These toolkits, however, are underutilized.[58] Moreover, the fact that *so many* organizations like NIST exist suggests that information exchange is not universally adopted, emphasizing the ambiguity within the ERC.

In addition to a lack of coordinated action across disciplines, Kello adds that technology advancements are being outpaced by our ability to understand their impacts.[59] Existing collaborations often narrow their focus to known threats such as the vulnerability of databases managed by NIST. Coordinated action requires cross-sector collaboration that addresses not only current threats, but also

emerging threats as well as the development of scenarios to help manage uncertainties across a range of future outcomes.

From an economic standpoint, a reduction in an environment's uncertainty improves profit stability which in turn has the potential to raise capital. In other words, information exchange has a positive influence on economic growth as a result of the "direct effect of better information on decision making [which] outweighs the competitive effect of letting rivals have access to one's own private information."[60]

Information exchange also fosters unity of effort towards a common goal. Unity of effort enables the synchronization of regime stakeholders across the ERC. Within the DOD, established command relationships are designed to facilitate the effective employment of cyber capabilities using various global, steady-state, combat-support, and contingency units which, when combined, constitute the bulk of U.S. cyber-related capabilities.[61] These cyber capabilities achieve unity of effort through two means: unity of command and cooperation with partners. The degree to which unity of effort is effective depends upon the manner through which it is achieved.

Unity of effort through unity of command is most effective.[62] Absent unity of command, fog and friction are introduced. A notable example is the separation of the Pacific theater during WWII into two separate theaters resulting from what Milan Vego, a professor of operations at the U.S. Naval War College, described as "parochial political reasons."[63] This led to the establishment of the Pacific Ocean Area, under Admiral Chester Nimitz as well as the Southwest Ocean Area, under the command of General Douglas MacArthur. The arrangement led to resource competition and often required arbitration from higher level authorities, including the President.[64] Similar issues arise in today's cyber substrate.

Some may argue that current unity of effort challenges can be resolved through Command & Control (C2) restructuring. In fact, extensive work analyzing the organization of C2 has resulted in an

exhaustive compendium of C2 alternative courses of action ranging from a stand-alone U.S. Cyber Force to a functional cyber component command.[65]

Cooperation is the other means of achieving unity of effort. Unfortunately, cooperation is overshadowed by competing principles such as safeguards. This past May of 2017, news reports surfaced describing debate over a 2016 U.S. Cyber Command OCO mission named Operation GLOWING SYMPHONY designed to degrade and disrupt ISIS communications on social media sites. While the mission was a success, challenges surfaced that it carried the operation out on computers located on foreign soil without notification to the other nation. Admiral Michael Rogers, the Director of the National Security Agency and Commander of U.S. Cyber Command recently commented on some of the difficulties. The challenge, Admiral Rogers subsequently noted, is that with offensive cyber operations, by informing your operation you reveal your capability, subsequently rendering the technique obsolete and causing the target to maneuver elsewhere.[66] Despite these security challenges, the principle of cooperation is crucial to ensuring strong linkages across the ERC.

Governance

Governance refers to the actions, processes, leadership, and institutions by which authority is exercised and informed decisions are implemented.[67] Two aspects of governance are crucial: risk governance and cyber governance. Risk governance applies the principles of governance to the understanding and management of risks in the context of the ERC.

The International Risk Governance Center defines risk as "the uncertainty about and severity of an event with respect to something valued."[68] More simply put, the International Organization for Standardization defines risk as the "effect of uncertainty on objectives."[69] Uncertainty pertains to both the likelihood of an event occurring, the type of impacts, the severity of its consequences, and the time when these consequences may occur.[70] The ERC employs this definition of risk because it

accommodates both positive and negative outcomes to include opportunity, hazards, and threats. Moreover, since risks are increasingly systemic and cannot be managed through the actions of a single person or group. Instead, due the complexity of the ERC, systemic risk requires involvement at the local, regional, national, and international levels with stakeholders from multiple disciplines.[71]

The ERC distinguishes between two risk framework pillars: understanding a risk and deciding what to do about a risk. Understanding is the generation and evaluation of knowledge.[72] Understanding relies heavily on the use of quantitative data to establish a risk appraisal resulting in an approach that focuses on past information to make an assessment about future risks. In contrast, deciding is qualitative and centers on judgement-based subjectivity. Deciding is fundamentally future leaning. Using John Boyd's decision-making process known as the OODA (Observe-Orient-Decide-Act) Loop[73], 'understanding' is synonymous with observation and orientation, whereas 'deciding' is in line with Boyd's decide and act phases.

In contrast, cyber governance applies the principles of governance beyond risk to the entire substrate. A subcomponent of cyber governance is Internet governance and includes both government organizations as well as non-governmental organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) which has the mandate of assigning top level numeric addresses.[74]

Lucas Kello articulates three increasingly prevalent characteristics affecting governance resulting from what he describes as "the Sovereignty Gap."[75] First, non-state actors are increasingly threats to national security. Second, non-state actors increasingly contribute to national security. Third, a nation-state's ability to control conflicts is no longer apparent.[76] Furthermore, due to the complexity, uncertainty, and ambiguity of risk across global systems it is increasingly difficult for stakeholders to respond alone.

Additionally, some ERC stakeholders responsible for cyber governance do not sufficiently address failure of compliance and rely too heavily on voluntary participation such as with U.S. Executive

Order 13636.[77] In these instances ERC stakeholders are caught between promoting democratic values, fostering economic growth, and providing security of critical infrastructure which may be vulnerable to cyber-attacks. Fulfilling these tasks requires cybersecurity governance to balance between government oversight and self-regulation. While voluntary, consensus-based governance must be considered as a valid component of the ERC, the breadth, uniqueness, and varying circumstances of organizations insist upon cyber governance designed to ensure that the legal system fosters communication across the ERC.

Cyber governance is also challenged with what some experts refer to as the balkanization of the internet, where ambiguity causes fragmentation amongst ERC stakeholders.[78] One means to prevent fragmentation and foster acceptance of voluntary, consensus-based governance is to provide effective incentives, such as extending grants, offering public recognition, and assigning preferential treatment in the tax code. On a case by case basis, additional incentives may include liability protections for disclosed information and Freedom of Information Act request exemptions,[79] but such actions require specific action by Congress.

Elsewhere across the ERC, where incentives prove insufficient or are inappropriate, cyber governance should take the form of regulation. Authority for government oversight of roles and responsibilities for organizations including those in the cyber substrate is derived from US Constitution and Federal law. Key statutory authorities pertaining to cybersecurity include: Title 6, United States Code (USC), Domestic Security; Title 10, USC, Role of the Armed Forces; Title 18, USC, Criminal Code; Title 32, USC, National Guard; Title 40, USC, Public Buildings/Properties/Works; and Title 50, USC, Role of War and National Defense.[80] Additionally, key Presidential Policy Directives are PPD 20, 21, 28, and 41.[81]

While this paper argues that cyberspace is a domain, when considering regulations, it is helpful to consider the fact that cyber is formally designated one of five domains, the others being land, sea, air, and space. All four other domains already have extensive regulation that deal with security and privacy

issues. Moreover, one could even argue that the authority for regulating both cybersecurity and, more specifically, computer code, already exists from a legal perspective. The Data Quality Act (DQA) provides government guidelines that "provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies." Although the DQA was a rider to the 2001 Consolidated Appropriations Act,[82] the guidelines provide a legal basis for implementing government regulation on government agencies. While this law only applies to government agencies, this provides precedent regarding regulation on the cyber substrate.

This differs however, from previous ideas pertaining to regulation in cyberspace. At the turn of the century, the 2003 National Strategy to Secure Cyberspace stated:

> *"Federal regulation will not become a primary means of securing cyberspace. Broad regulations mandating how all corporations must configure their information systems could divert more successful efforts by creating a lowest-common denominator approach to cybersecurity, which evolving technology would quickly marginalize. Even worse, such an approach could result in less secure and more homogeneous security architectures than we have now. By law, some federal regulatory agencies already include cybersecurity considerations in their oversight activity. However, the market itself is expected to provide the major impetus to improve cybersecurity."*[83]

ERC stakeholders must also be cognizant that a regime can be highly regulated as well as highly vulnerable. An example of this is evident upon further review of the health care industry. The 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act (which included the Federal Security Management Act (FISMA)) all dictate cybersecurity specific regulations, but despite this the industry remains vulnerable in part due to the lack of other principles such as technical safeguards.[84]

One area where the use of government regulation should be mandatory is national security. Regulation should be implemented as part of a holistic cybersecurity strategy when vital national interests necessary to maintain a functioning government are at risk to include the following sectors:

Critical national infrastructure sectors as defined by Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience; additional critical government infrastructure as defined by the Department of Homeland Security; and additional critical military infrastructure as defined by the Department of Defense.

The US Government's definition of *critical infrastructure,* however, is broad and loosely defined. Left alone the definition lacks meaning because it doesn't provide the specificity necessary to provide guidance for corporations. This is significant since the private sector controls nearly 90% of the US critical infrastructure.[85]

Ever since Presidential Decision Directive 63 (PDD-63) was produced on May 22, 1998, (which drew from the President Clinton Commission on Critical Infrastructure Protection) government documents have communicated recognition that America's military and economy were "increasingly reliant upon certain critical infrastructures and upon cyber-based information systems."[86] Since, then the US government has continued attempts to better address cybersecurity related issues pertaining to critical infrastructure. EO13636, follows in this vein, but fails to provide clarity.

In today's world, critical infrastructure is pushing further into 'global commons' territory. For example, undersea cables are not considered part of US critical infrastructure even though they are responsible for transporting 95-98% of the world's telecommunications traffic.[87] Although sea cables are protected under the United Nations Convention on the Law of the Sea (UNCLOS) Article 113, this still falls under International Peacetime law, not *domestic law*. Adding to the ambiguity and complexity is the fact that although the U.S. recognizes the UNCLOS a codification of customary international law, it has not yet ratified the treaty.

National organizations such as the North American Submarine Cable Association (NASCA), a collection of 16 North American based companies which advocate on behalf of the Undersea Cable Industry as well as international ventures such as the North America International Cable Protection

Committee (ICPC), comprised of over 100 companies and 50 countries[88] require better integration and access to sustainment capabilities to bridge the gap between national and international assets vital to our nation's critical infrastructure.

Another alternative is to bypass this issue altogether. For example, many senior government officials have advocated for a more secure form of internet, by constructing independent and trusted networks "inside the Internet." General Keith Alexander, former head of both the NSA and Cyber Command, argued for a "secure, protected zone." Additionally, the FBI's former Assistant Director Shawn Henry argued for a "new highly secure alternative Internet."[89]

Safeguards

The safeguarding of US national interests requires a cybersecurity strategy that is implemented across the whole-of-society. It requires continuous engagement among stakeholders to ensure a balance between security and privacy for individual users. While individual technical safeguards are important, in the strategic context of the ERC, legal safeguards pertaining to offensive and defensive actions are crucial. Already, the structure of many national cybersecurity strategies within the ERC includes offensive and defensive operations. In the U.S., national defense safeguards include, Information Network Operations (DODIN Ops), Defensive Cyber Operations (DCO), and when called upon, Offensive Cyber Operations (OCO). Combined they bring offensive, defensive, and exploitation capabilities to bear on cyber threats.[90]

Several strategic gaps in the resilience of our national critical infrastructure remain, however, and due to the ubiquitous nature of the Internet, safeguarding must be considered in the global context of the ERC. This has proven to be extremely difficult as can be demonstrated by the fact that from an international sovereignty perspective, no treaty is associated with cyberspace. Unlike the space domain, which is governed by the 1967 Outer Space Treaty restricting military activity,[91] the absence of legal

restraints prohibiting the use of cyberspace for military use enables offensive operations. Determining when, how, and to what extent a stakeholder can act is difficult in part because there is no precedent.

Another strategic safeguard gap relates to the Law of Armed Conflict (LOAC), as it pertains to cybered-conflict. The LOAC, also referred to as the law of war[92] or international humanitarian law, is deeply rooted in history and regulates the conduct of warfare not the prevention of it. The LOAC emerges from a desire among nation states to prevent "unnecessary suffering" of personnel and/or destruction while still "permitting the use of force."[93] This is because the LOAC recognizes that to prevent unnecessary death and destruction the effective waging of war must not be hindered. More specifically, the LOAC pertains to the means and methods of hostilities, more commonly known in legal terms as the jus in bello. This can also be stated as *how* force can be used once hostilities have begun. *When* states can use force, or the jus ad bellum, is not specifically addressed. When first written, the LOAC did not consider cyber operations, however.

Michael Schmitt, principle author of *Tallinn 2.0: On The International Law Applicable To Cyber Operations,* proposes a multi-factor test to determine when a cyber-attack is an armed attack. The "Schmitt-test" as it is known considers seven elements when an armed attack has occurred: severity, immediacy, directness, invasiveness, measurability, presumptiveness, legitimacy, and responsibility. One interesting distinction he makes is between the terms "use of force" and "armed attacks." While these terms are well established within the LOAC, he makes specific points relating to cyber in that an armed attack may be cyber or kinetic. This is a fundamental shift in traditional Law of Armed Conflict thinking because it expands upon the idea of what constitutes a weapon.[94]

Safeguarding in the form of responding to an attack is not without its limitations, however. Most stakeholders do not have access to offensive means and they are limited to what can be done defensively. Even when an attack is determined, there is limited legal recourse by which a stakeholder can respond to an attack outside their own boundaries.

Rather than limiting the range of attack responses by non-state actors to strictly conventional defensive measures which do not extend beyond the boundaries of the organization, safeguarding must allow for these actors a degree of active defense. According to Schmitt, a preeminent attack, or active defense, is "the last feasible window of opportunity for self-defense in the face of an [actual armed] attack that was almost certainly going to occur."[95] Criteria for determination is predicated upon three factors: Capability (can they attack you?); Intent; and Final Opportunity (the last moment at which an actor can defend itself and were they to wait longer to act, it would be too late).

Active defense as a form of deterrence is increasingly necessary in an environment consisting of low cost of entry for offensive operations. Because capability, intent, and final opportunity are subjective, some initiatives are developing a legal basis by which non-state actors may conduct active cyber defense under certain conditions. The complexity of the issue demands the integration of like-minded organizations within the regime complex when civil and criminal oversight organizations such as the FBI and DOJ can exhibit control and limit the response of other stakeholders conducting active defense. One such measure is the Active Cyber Defense Certainty Act (ACDC), H.R. 4026, which is a bipartisan bill proposing changes to the Computer Fraud and Abuse Act (CFAA). The bill, introduced by Reps. Tom Graves (R-GA-14) and Kyrsten Sinema (D-AZ-09) on October 13, 2017, gives authorized individuals the legal authority to proceed beyond their own network for the purposes of determining attribution, disrupting cyberattacks, monitoring behavior of an attacker, and the retrieval of stolen files.[96]

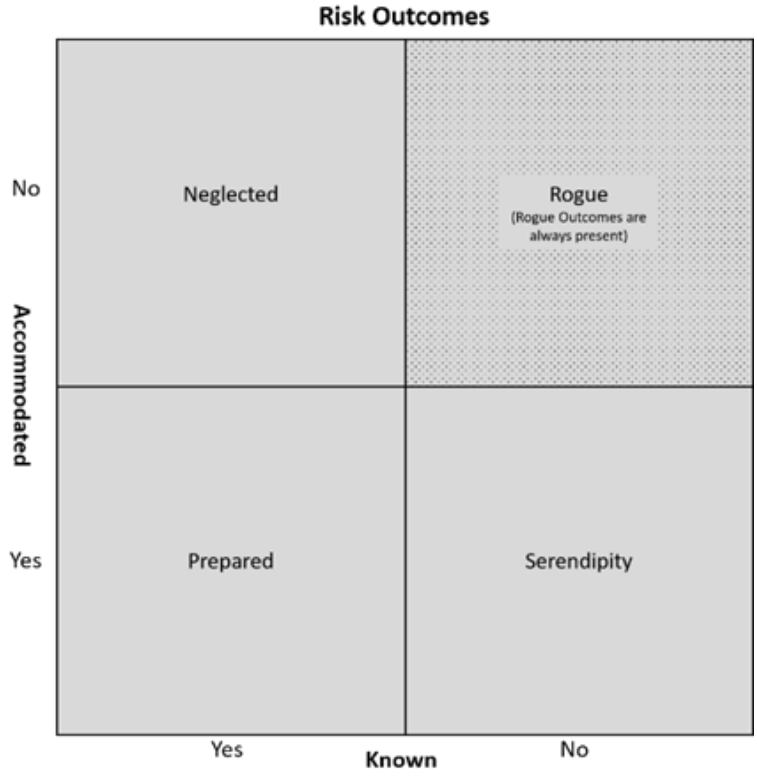
Additional safeguards may come in the form of compensation after an event has occurred. Indemnification, or the guarantee to provide compensation over a loss that has already taken place, is another useful tool to compliment other safeguards and can be implemented using both state and non-state actors (e.g. government guarantees or cyber-structured insurance policies). The linkage between government and non-government agencies is critical since measures must be in place to account for

situations that overwhelm insurance compensation due to damages, much as they are in the physical world during times of extraordinary crises. Cyberspace has the potential to exacerbate these kinds of problems exponentially.

Part IV:
Enablers

Standards, stakeholder engagement, communication, unity of effort, strategic context, and education all provide linkage between various ERC stakeholders. Except for education, the enablers listed here have been previously discussed directly and indirectly in the body of this paper. Education is a key foundation for the rest as it fosters innovation, which in turn promotes growth and prosperity.

Figure 4: Decision Outcomes



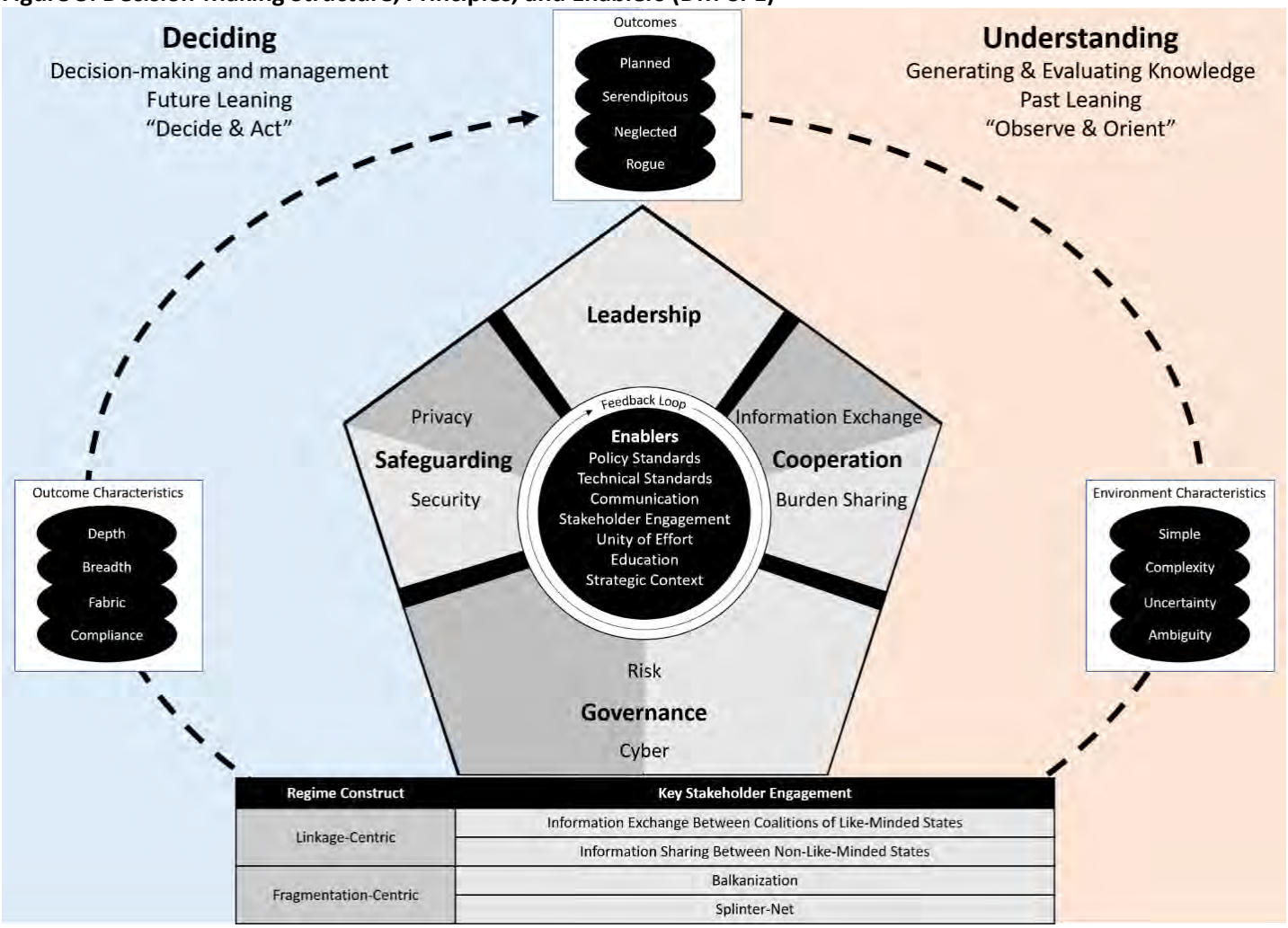
Source: Developed by author and derived from Chris Demchak, lecture on March 16, 2017, "Complexity, Cybered Conflict, and Socio-Technical Systems' Surprise," U.S. Naval War College.

Decisions by policy makers, legislators, and senior leaders must be based on up-to-date knowledge of the state of cybersecurity. Education is the key to developing understanding, ensuring the transfer of knowledge, and making informed decisions. It is the key enabler for impacting decision outcomes in the long term. Decision outcomes can result in four possibilities: prepared, serendipitous, neglected, and rogue (Figure 4). Each outcome is a function of the degree of knowledge relative to the degree of accommodation. A high degree of knowledge with a corresponding high degree of accommodation leads to decisions which result in prepared outcomes. In contrast a high degree of knowledge with a low degree of accommodation, implies an agnostic degree of neglect to the outcome. Rogue outcomes are always present but decrease with a corresponding increase in education.[97]

Education

Education is critical in this regard because it affects both axes. The level of knowledge generally increases with more education while the degree to which a decision-maker addresses an issue is affected by a decision-makers understanding of the strategic context. The strategic context varies based upon the degree of understanding of an issue. Because of the impact education has on decision outcomes resulting from the ability to enable ERC stakeholder understanding of the strategic context, education serves as a key linkage between understanding and decision-making and helps with heuristics (see Figure 5).

Figure 5: Decision-Making Structure, Principles, and Enablers (DM-SPE)



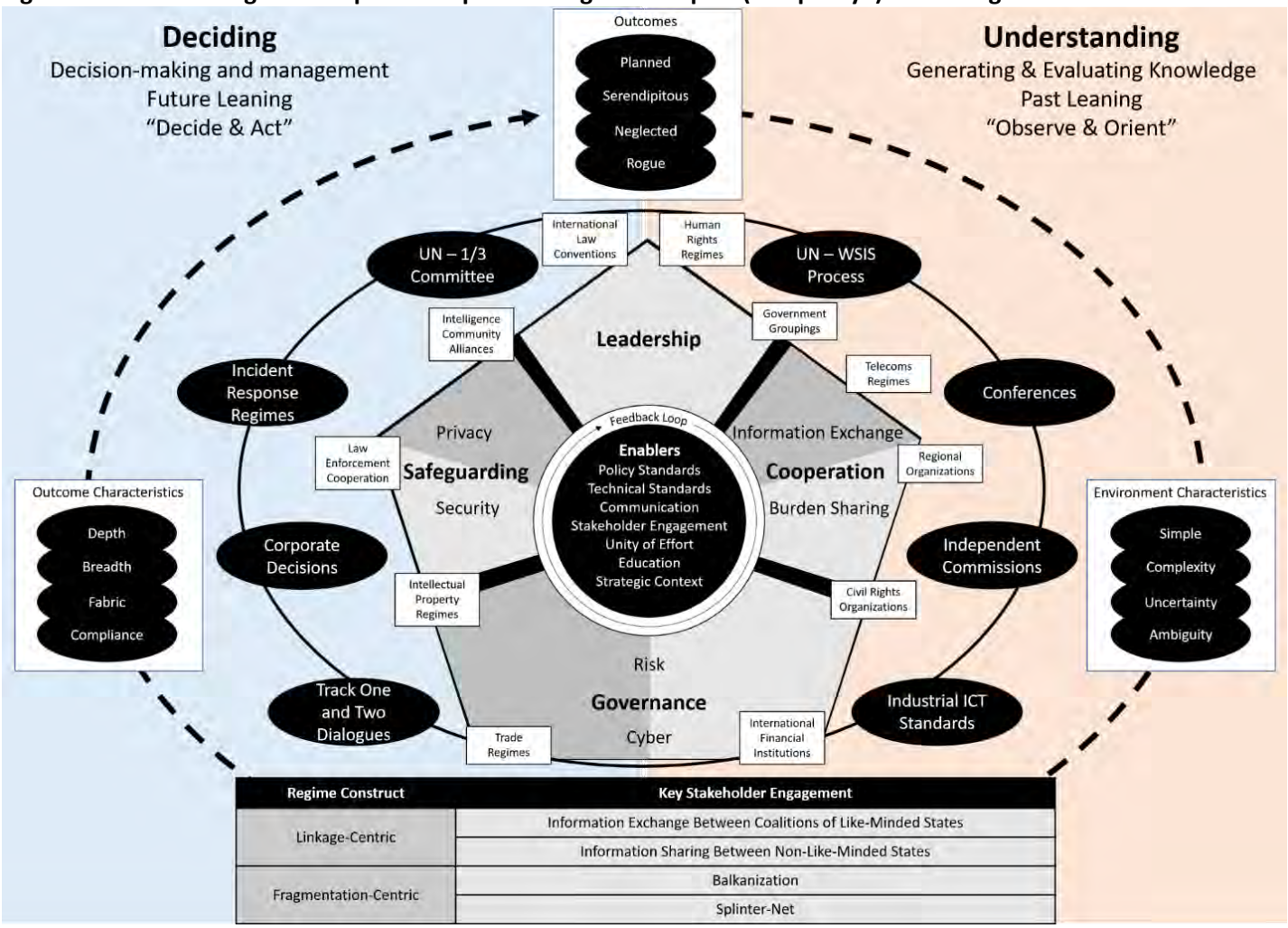
**Sources: Developed by Author with the following additional references: "Depth," "Breadth," "Fabric," "Compliance," and Key Stakeholder Engagement Types are derived from Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014); "Simple," "Complexity," "Uncertainty," and "Ambiguity" are derived from IRGC, "Introduction to the IRGC Risk Governance Framework," revised version 2017, (Lausanne: EPFL International Risk Governance Center); "Planned," "Serendipitous," "Neglected," and "Rogue" are from Chris Demchak, lecture on March 16, 2017, "Complexity, Cybered Conflict, and Socio-Technical Systems' Surprise," U.S. Naval War College.*

Continuous learning allows some stakeholders to acknowledge failure as part of a successful process rather than merely an undesirable outcome. From a scientific perspective, education imbues researchers with the notion that temporal failures are a function of the learning process.

Additionally, research to address Internet weaknesses will lead to technological advances and changes in methodology. For example, the Information Technology Labs at NIST provide a working

compilation of best practices for daily operations by combining existing corporate standards to form improved standards. Elsewhere, the National Security Agency's *Information Assurance Directorate: NSA Methodologies for Adversary Obstruction* methodology is based upon the "preposturing [of] defensive capabilities" with the goal of "impeding the objectives of a potential the intruder." [98]

Figure 6: Enhanced Regime Complex Incorporates Regime Complex (Joseph Nye) with Integrated DM-SPE



Regime Construct	Key Stakeholder Engagement
Linkage-Centric	Information Exchange Between Coalitions of Like-Minded States
	Information Sharing Between Non-Like-Minded States
Fragmentation-Centric	Balkanization
	Splinter-Net

**Sources: Developed by Author with the following additional references: "Depth," "Breadth," "Fabric," "Compliance," and Key Stakeholder Engagement Types are derived from Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014); "Simple," "Complexity," "Uncertainty," and "Ambiguity" are derived from IRGC, "Introduction to the IRGC Risk Governance Framework," revised version 2017, (Lausanne: EPFL International Risk Governance Center); "Planned," "Serendipitous," "Neglected," and "Rogue" are from Chris Demchak, lecture on March 16, 2017, "Complexity, Cybered Conflict, and Socio-Technical Systems' Surprise," U.S. Naval War College.*

Part V:
Challenges

Cyber Legibility

Cyber legibility underscores the importance of what Wayne Hughes described in his six cornerstones on Fleet tactics: "[People] matter most."[99] Cyber legibility describes the degree to which factors pertaining to cyberspace are understood by those whose actions within the ERC requires a degree of fluency. Challenges to cyber legibility include factors such as lexicon used across varying regimes, what constitutes cyberspace, and key terrain in cyberspace.

First, cyber lexicon is maturing. Joint Publications such as JP 3-12 on cyberspace operations and service specific manuals like the recently published Army Field Manual (FM) 3-12 on Cyber and Electronic Warfare Operations provide clear definitions to relevant cyberspace terminology. Still, cyber terms are often either too technical or too fledgling to be universally understood, limiting their usefulness when applying the vernacular of cyber to the ERC. Elsewhere, domain overlap has the potential to confuse planners due to the difficulty involved in explaining cyber concepts across the complex, uncertain, and ambiguous ERC. JP 3-12 recognizes this point to the extent that a portion of the document pertains directly to the complex nature of domain overlap.[100]

Training and education improves understanding and proficiency, but due to a lack of interaction with career professionals who often work in remote secure facilities, cyber legibility is degraded. Subsequently, without the means to support use of a cyber lexicon, actors within the ERC may neglect the cyber substrate entirely. Increasingly, the absence of cyber in planning proves less about lack of

recognition and more about personnel who simply don't know how cyber operations should be applied. This failure results in the omission of key considerations such as key terrain in cyber. In the physical world, when crucial parts of planning are overlooked, the penalty is often severe. The same holds true in the cyber substrate.

Second, as this paper has already pointed out, defining cyberspace as a domain is confusing and limits universal understanding. JP 3-12 defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[101] The DOD currently uses the term 'cyber domain' to account for all operations within cyberspace. This term was first utilized by the United States Air Force to assist in classification coinciding with existing frameworks and to align cyberspace with air, land, sea, and space domains.[102] Accordingly, applied in this manner the concept of a cyber domain is used for administratively convenient purposes because it fits within the operational construct alongside other, physical domains.

Alternatively, a term that better encompasses cyberspace is the word 'substrate.' Chris Demchak and Peter Dombrowski of the U.S. Naval War College first used this term to account for the persistent, pervasive, and ubiquitous nature of cyberspace.[103] Elsewhere, Joseph Nye uses the term substrate to describe the Internet.[104] Unlike a domain, whose limits are well defined, cyberspace as a substrate resembles a sort of digital petri dish, which serves as an environment in which other things can grow or are attached. The Cyberspace substrate exists across all domains. For example, the only way for operational commanders to interact with the space domain is through the cyber substrate. Once again, the distinction between substrate and domain is relevant to the ERC because it affords key stakeholders a more accurate depiction of cyberspace and improves cyber legibility as it relates to

operational space. Additionally, as previously discussed, the pervasive nature of the cyber substrate requires a measure of understanding of the entire panoply of domains that other domains do not.

Some may argue that the distinction is irrelevant because the cyber domain encompasses additional aspects that the cyber substrate does not. Most notably, while cyberspace can exist within a cyber domain, a cyber domain cannot be entirely encompassed by cyberspace, a fact that would seem to reinforce this counterargument. Cognitive and physical factors, such as the law and the geographic location of Cyber Command, do not fall within the substrate, but are relevant to the cyber domain. Understandably, the benefits of aligning cyberspace with existing domains streamlines operational planning.

Moreover, the distinction demonstrates that a substrate has characteristics that domains typically do not. First, factors such as attribution, speed, scale, and precision are more pronounced in the cyber substrate, as opposed to the rest of the cyber domain, where elements are more loosely coupled resulting in actions occurring at reduced speeds and to lesser degrees. Finally, although the nature of warfare remains unchanged, the conduct of war within the cyber substrate requires an unprecedented degree of interaction, caused by the pervasive malleability inherent to the cyberspace substrate. While cyberspace is also limited by physical properties, in this case pertaining to the electromagnetic spectrum, the substrate is unique insofar as it persists across all domains. Key stakeholders must think of cyberspace as a substrate to more readily understand the risks, both positive and negative. Reclassifying what cyberspace is affords actors within the ERC the opportunity to apply regime theory and strategy more effectively by recognizing what makes the substrate fundamentally different rather than as a measure of administrative convenience.

Finally, the third factor affecting cyber legibility is key terrain in cyberspace. Key terrain includes those aspects of the surrounding landscape that can have a significant impact on the outcome of decisions within a given environment. Key terrain can be contested, but it can also vary amongst

different stakeholders. Key terrain facilitates determination of decisive points. Antoine-Henri Jomini described permanent decisive points as the "topographical and strategic descriptions of the theater of war,"[105] but key terrain in cyberspace is inherently different. Actors within the ERC use terrain to their advantage by avoiding friction points, known as surfaces and exploiting opportunities or weaknesses, known as gaps. Key terrain is even more important because it is comprised of several decisive points that can facilitate actions resulting in the control of the surrounding environment. In military terms, actions on decisive points are conducted to emerge victorious over enemies, hence the use of the word 'decisive.' Differences in cyber key terrain exist across the physical, logical, and cyber-personas.[106] Essential differences pertain to the technological complexity of the substrate resulting in the need for strong cyber legibility to best understand the nature of the space and the elements within.

Some may argue, key terrain in cyberspace is best described in relation to the physical location of the asset being determined. FM 3-12 states operational planners must consider the nature of enemy cyberspace utilization and direct planning staffs to consider key terrain in relation to the physical locations within the area of interest.[107] In this example, however, FM 3-12 is referring to weather, and it's influence on the virtual world. The development of cyber legibility requires operational planners and their commanders to distinguish physical key terrain from key terrain in cyber. The concept of cyber key terrain (C-KT), emerged from the U.S. Naval War College War Game titled CYBER FLAG 15-1 and ties the operational factor of space together with CO.[108] Discernment between physical and C-KT is important in the planning process to identify new and advanced threats such as malware code like Stuxnet. Although Stuxnet targeted specific physical sites, its location wasn't bound to a physical space.[109] Key terrain would most certainly include points of entry, means of transmission, and the relationship of the industrial control systems to the physical world. Determining key terrain in cyber, however, requires more than cyber legibility. It also requires assistance with blind spots resulting in the need for cooperation and unity of effort.

Unity of Effort

Unity of effort, or the harmonization of multiple entities towards a common objective, has yet to be achieved in a way that enhances effective cybersecurity. While a patchwork of cybersecurity initiatives exists nationwide, ranging from best practices to incident notification, many if not most of these initiatives work independently of each other. Moreover, when collaboration between organizations does occur, the results of such initiatives often vary, since many of these lines of effort are predicated upon voluntary participation. Unity of effort in cybersecurity as described earlier in this paper will only be effective when the collective self-interest of organizations within the diplomatic, informational, military, and economic (DIME)[110] environments align.

Self-interest is defined as one individual's impulse to maximize gain. Collective self-interest is the maximization of gain for multiple groups and can be achieved either intentionally, or unintentionally. Writer Ayn Rand suggested in her objectivist philosophy that self-interest was rational since it benefits both the individual and society in the long run. In this regard, collective self-interest is achieved unintentionally as a bi-product of individual self-interest.[111] In cybersecurity, individual self-interest is mutually beneficial due to the degree of computer interconnectivity. Data across a network is more secure when every individual works to protect their data. Similarly, the system of networks is more secure if each network strives for better security collectively.

Alternatively, collective self-interest can be achieved intentionally, through deliberate actions from individuals and organizations purposefully aligned with the interests of society. This concept, known as enlightened self-interest, originated in the writings of democratic and free-market thinkers such as economist Adam Smith[112] and diplomat Alexis de Tocqueville[113]. Their philosophies suggest that individual circumstances will improve for all organizations if they respond to the interests of society. Today, enlightened self-interest is generally referred to as corporate social responsibility.[114]

Corporate social responsibility has the potential to achieve enlightened self-interest or what Benjamin Franklin called a means to "do well by doing good,"[115] however, this approach is flawed for two reasons. First, much like an uninhibited government, neither individuals nor organizations are angels and there is always a risk that one interest will seek precedence over others.[116] Second, actions taken under the guise of corporate social responsibility are mostly voluntary and require substantial efforts over time.

The first problem can be solved by ensuring that no one interest has inordinate power. The danger of lobbying, without corresponding government inputs, however, is that cybersecurity decisions can be outsourced to the highest bidder. As recently as 2013, for example, lobbyists spent $3.24 billion for the opportunity to promote their interests to Congress.[117] Lobbyists with little opposition can achieve their goals, but often at the expense of others.

Encouraging the proliferation of interest groups is one way of limiting power. The greater the number of interest groups present, the less likely it is for any one interest group to dominate within the DIME environment. Lobbying proves more difficult because the chance for marginalization of other groups is reduced.[118]

The second problem pertaining to the voluntary nature of corporate social responsibility and enlightened self-interest can be solved through the application of laws. Government cybersecurity laws provide a means to assure collective self-interest by imposing constraints, or things organizations must do; and restraints, things organizations must not do. Many states recognize the need to implement cybersecurity laws at the state level, for example, with their implementation of data breach laws. Due to the ubiquitous nature of the Internet, however, data breach laws at the state level are insufficient. While they are tied to lines on a map, the Internet does not adhere to the same geographic limitations.

One recent initiative is aimed at resolving some of the inconsistencies of state laws. On September 18, 2017 Congressman Jim Langevin (D-RI) reintroduced a bill in the US House of

Representatives labeled The Personal Data Notification Act of 2017.[119] The proposed bill seeks to achieve unity of effort and clarity by replacing existing breach notification laws, which currently consist of 48 separate state laws, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, with a nationwide standard.[120]

Achieving a unified standard, however, is wrought with logistical, political, and economic challenges. Many states may resist a national law that adversely impacts their constituents in the near term. Interest groups may also weigh in through intense lobbying actions similar to what occurred in 2015, when credit bureaus sought to undermine the original bill's goals for fear that reforms would hurt their bottom line.[121]

Despite these challenges, a federal data breach law is necessary. First, it would ensure that no single interest group or state has excessive power that adversely affects other organizations. Second, it reinforces unity of effort to achieve effective cybersecurity. Federal mandates can require information sharing and analysis in line with existing Department of Homeland Security recommendations while private organizations can lobby to ensure that their own self-interest is preserved in the process.[122]

Implementation of a federal data breach law may require federal government involvement. Maintenance of such laws over time, however, should be facilitated by both government and non-government organizations, which will receive mutual benefits. In other words, unity of effort in cybersecurity can be achieved initially through unintentional objectivist self-interest, and subsequently through intentional enlightened self-interest within the Diplomatic, Informational, Military, and Economic (DIME) environment. Evidence of a government achieving unity of effort by first imposing laws that will eventually lead to a shared mutual understanding of collective self-interest can be found in Estonia.

When Estonian president Kersti Kaljulaid spoke during a NATO cyber-conference in Tallinn in June 2017, he referenced Carl von Clausewitz's famous statement: "'war is a continuation of policy by

other means'," adding in his own words that "every country should have a cyber war."[123] Kaljulaid was referring to recent cyberattacks initiated from Russia in response to Estonia's removal of a Soviet statue in Tallinn.[124] Although Kaljulaids's comments were far from reserved, he did have a point. Exposure to cyber conflict at the national level provided Estonia the necessary impetus to further cybersecurity initiatives and resulted in a nation-wide effort to strengthen cybersecurity. Estonia's efforts were so successful that cybersecurity became part of ordinary citizens' national identity. Furthermore, the story of Estonia as a cybered nation stands as a testament that, given the right circumstances, individuals across a country will educate themselves in cybersecurity awareness when it is in their best interest to do so.

Unity of effort in cybersecurity will only be achieved with the alignment of self-interest across the DIME environment. In response to the current patchwork of initiatives ranging from individual corporate best practices to state data breach laws, initial implementation of national cybersecurity laws will force the initial alignment. Over time, unity of effort will be maintained by the enlightened self-interest of individuals and organizations who will come to understand, as Alexis de Tocqueville once suggested, that "extraordinary virtues would doubtless be more rare; but I think that gross depravity would then also be less common."[125]

Planning

As Milan Vego of the United States Naval War College states, "the very essence of operational art is to win decisively in the shortest amount of time possible and with the least loss of human lives and material,"[126] but in order to achieve this objective, effective planning must be applied to cyberspace. This paper attests that solutions to *all* cyberspace-related challenges exceed the capabilities of any single planning process alone. Much like cybersecurity implementation, which requires a layered approach across all phases of operations, ERC planning should incorporate alternative methods to

ensure success. In order of implementation priority, three types of planning processes are worth considering: Strategic Management Scenarios, Operational Planning, and Modeling. Rather than using only portions of each, this syncretic approach uses all three processes fully for improved planning results. Fully merging multiple approaches works quite well. For example, NIST provides a working compilation of best practices for daily operations by combining multiple existing corporate standards to form improved standards.[127]

Strategic Management Scenarios

Problem framing is both backward looking and future leaning. Backward leaning refers to the use of quantitative data. Quantitative formulae are, by definition, backward looking since data can only be collected from the past and, because of this, quantitative data ignores novel strategies and novel threats (e.g. Panzer tanks crossing the Maginot Line could not have been predicted using available metrics at the outset of WWII).

Since risk cannot be accounted for using individual data points only, a future leaning approach must also be incorporated to describe the strategic construct. Future leaning refers to the use of a coinciding set of scenarios to develop a subset of actions across a range of events and plausible futures. Strategy scenarios offer a detailed description of a range of plausible futures and encourage the inclusion of qualitative judgement in risk and cyber governance early. Because of this, scenarios can only be used as a set and are distinct from both Courses of Action (COA) and Wargaming models. Wargaming is an event scenario and focuses on a specific future. Often, stakeholders attempt to identify the most likely COA after wargaming a specific future, but this does not fully consider the impact of world events and the ERC as whole.

Unlike COA or wargaming functions, strategic scenarios manage uncertainty by developing a subset of actions across a range of events, none of which are likely to occur, but each of which is

plausible at the margin. Although the probability of any one scenario is zero, as a set they embrace the likely range of possibilities. In contrast, if problem framing were to begin with numbers, thinking would automatically be narrowed. This is managing uncertainty.

Operational Planning

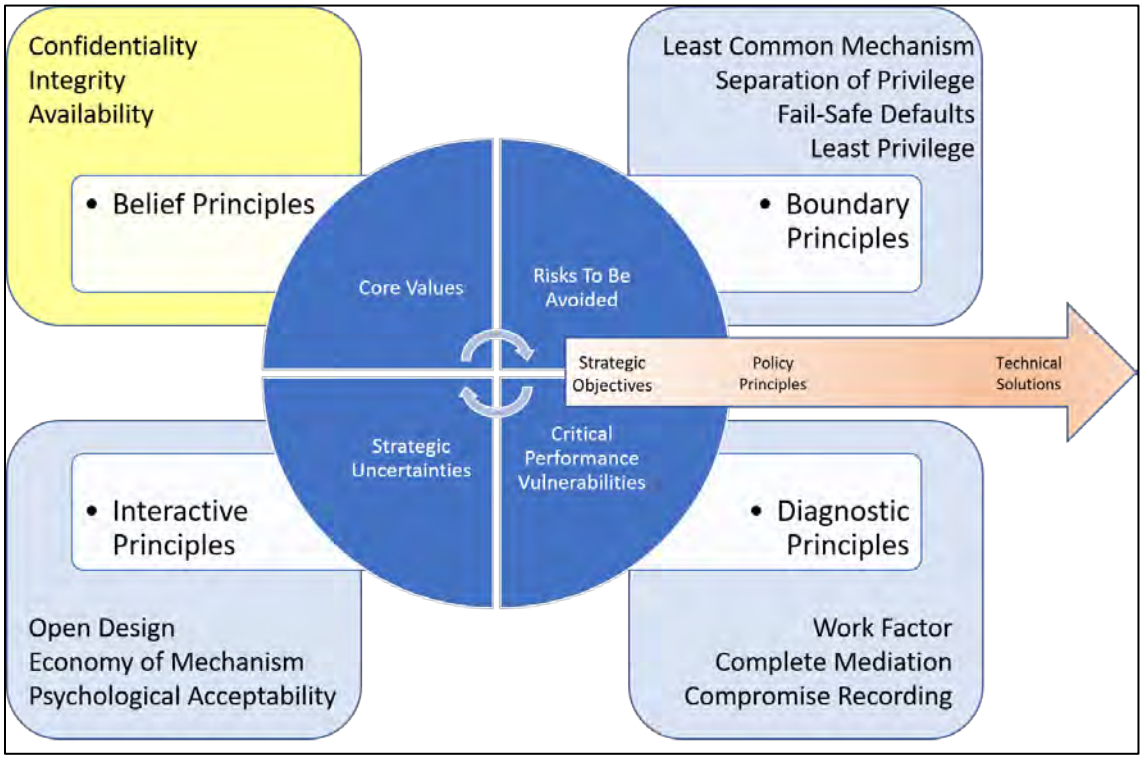
The military uses operational planning constructs to inform decisions in a complex, uncertain, and ambiguous environment. Admiral Michael Mullen prefaces JP 5-0, Joint Operation Planning, with recognition that the operational environment is temporal and requires adaptability and flexibility in the conduct of planning and execution.[128] JP 3-12, Cyber Operations aptly notes that cyberspace operations utilize the same planning considerations employed for use in planning other joint functions, but it makes an important distinction in that they also have some "unique considerations,"[129] without divulging their significance. Sometimes, these considerations are classified, which adds self-imposed friction into the planning process. Cyber operations planning is even more difficult when conducting operational planning with international partners because not only do security concerns limit synchronization between partnering countries, but the laws governing each nation-state may affect the willingness or ability to participate in cyber operations.[130] Even if Foreign Disclosure Officers, who determine which information may be reclassified, approve information for transmission to an international partner,[131] the time required to guarantee completion of this task relative to the requirement necessary for successful cyber operations is prohibitive.

Although some may argue that actions within the ERC require only current planning methods, certain characteristics of cyberspace require operational planners to at least consider alternative methods to augment existing planning methods. While the general approaches may appear similar, they often lead to drastically different results, which can subsequently be placed into various courses of action for commanders to decide among. Moreover, operational planning does not always account for

certain key aspects such as guiding principles and performance-based metrics as depicted in Figure 7, resulting in significant planning gaps. While certain increasingly sophisticated technological capabilities are available, such as artificial intelligence and machine learning, the intent is to provide low cost augmentations to existing planning tools, employable even when the lights go out.

The private sector's classic description for cybersecurity pertaining to computers and networks involves three fundamental concepts of confidentiality, integrity, and accessibility. These concepts are more commonly referred to as the CIA triad.[132] Like most doctrine drawing upon certain principles of warfare, the CIA triad is used to establish a security framework and informs tactics, techniques, and procedures used to scope out threats and protect assets. Using heuristics, operational planners map out their designs using various sets of criteria. An example of framing the environment using heuristics is depicted in Figure 7.

Figure 7: The Relationship Between Guiding Principles and Performance-Based Metrics Using Heuristics

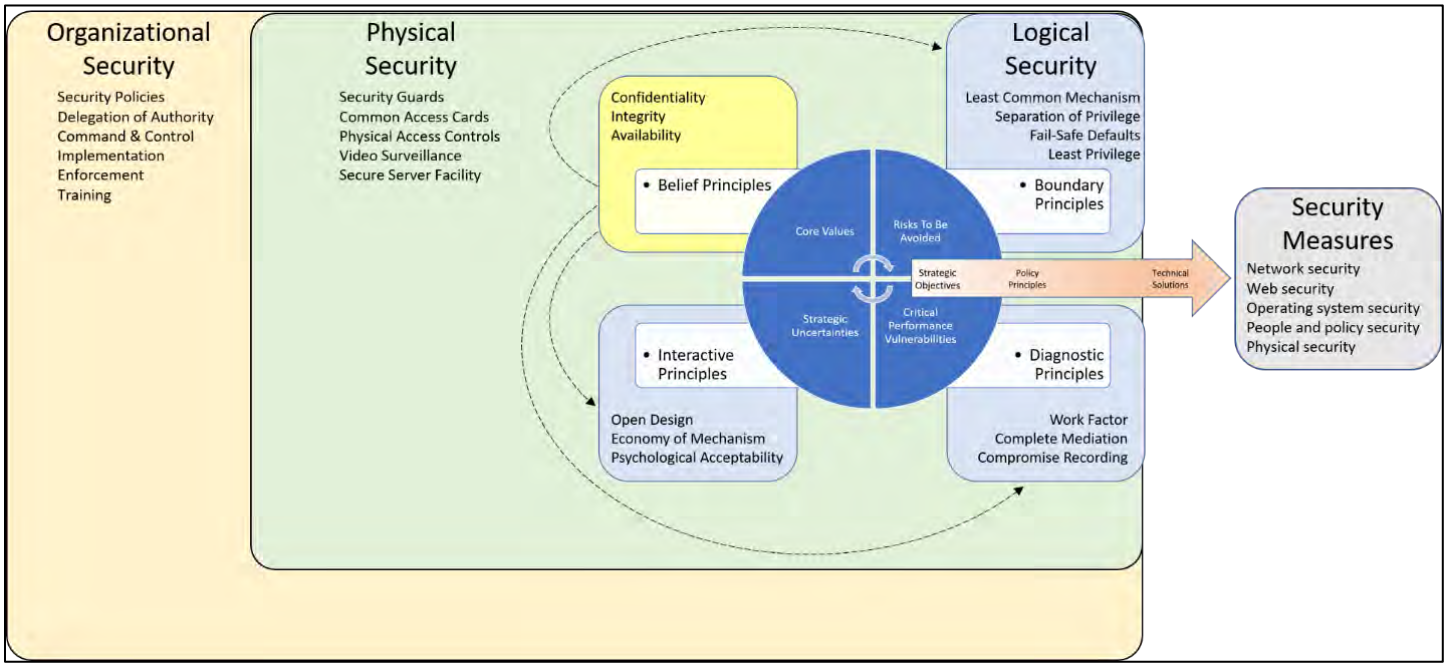


Sources: "Belief, Boundary, Interactive, and Diagnostic Principles" have been adapted from the Renew Strategy with the four levels of control by: Robert Simmons, "Control in an Age of Empowerment," Harvard Business Review, (March-April 1995), p.2. In this article, Simmons discusses metrics using four control measures: Belief,

Boundary, Interactive, and Diagnostic; The "10 Logical Security Principles" are from Saltzer, Jerome and Schroeder, Michael. The Protection of Information in Computer Systems. Proceedings of the IEEE, 1975, 63(9).

Confidentiality is, according to computer scientists Michael Goodrich and Roberto Tamassia, "the avoidance of the unauthorized disclosure of information,"[133] Within the DoD confidentiality is enforced using methods such data encryption, access control, authentication, and authorization, as well as a host of physical security measures. Goodrich and Tamassia define integrity, as a property that exists when information or data "has not been altered in an unauthorized way."[134] Examples of integrity include establishing a periodic data baselining program and data archiving. The goal of the integrity principle is to identify malicious activity and employ redundancy into the storage practices of the DoD. Finally, availability is the property in which, as Goodrich and Tamassia state, "information is accessible and modifiable in a timely fashion by those authorized to do so."[135] Establishing security clearances to individuals is an example of how the DoD might apply the concept of availability.

Figure 8: Developing a Construct of the Operating Environment to Identify Resource Shortfalls



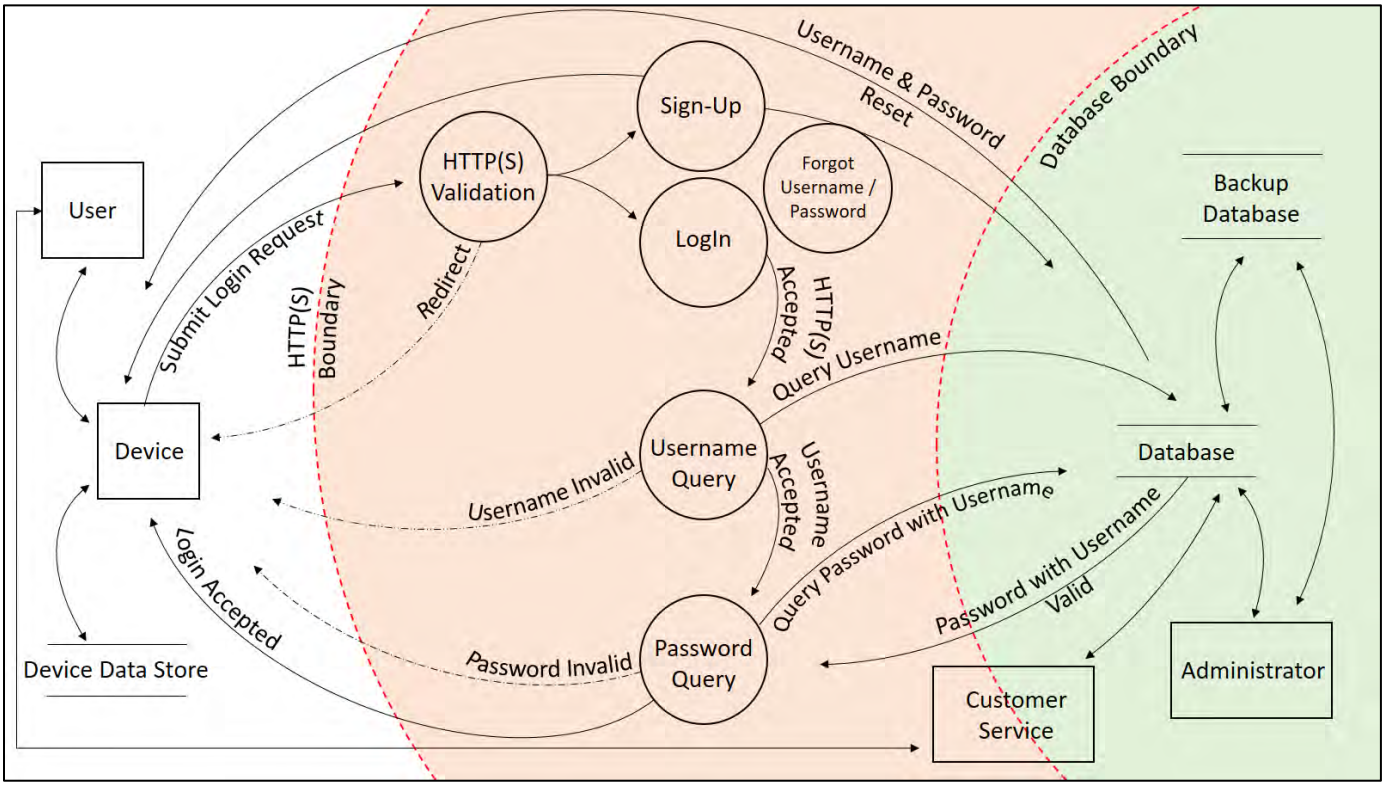
Sources: Ibid; Simmons, "Control in an Age of Empowerment," Harvard Business Review, (March-April 1995), p.2.

Using the CIA triad as a guiding principle, cybersecurity measures the fall into three broad categories: Physical, Logical, and Organizational.[136] (See Figure 8). Different types of security principles can be sub-categorized. In the example given using Figures 1 & 2, 10 security principles are listed in the three blue boxes. These principles are derived from Jerome Saltzer and Michael Schroeder's classic 1975 work titled, *The Protection of Information In Computer Systems*.[137]

Modeling

Following a logical flow, threat modeling developed through established alternative processes such as the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege)[138] method (Figure 9), will mitigate potential false alarms by considering threat vectors not normally associated with operational decision-making and planning.

Figure 9: STRIDE Model Example of a PDA Password Manager to ID Weaknesses and Determine Key Cyber Terrain



Source: Michael Perrottet, "Threat Modeling," EMCS Human Factors in Computer Security, 23 April 2017.

In the STRIDE model example given, potential vulnerabilities inherent to an individual's password manager on their personal device assistant (PDA) is sketched out. This example is chosen to emphasize the pervasiveness of the operating environment and the unlikelihood that current operational planning would identify such a threat. If a person stores their password on their PDA, several vulnerabilities are open to exploitation by potential adversaries. STRIDE modeling attempts to identify those vulnerabilities as well as likely enemy courses of action for a specific attack. Although this example involves only one individual, the methodology is scalable, and complimentary to existing planning assessment processes. These processes are not meant to replace, nor are they meant to be synchronized. Instead they are meant to run parallel to existing planning processes and identify potential vulnerabilities that might otherwise be overlooked.

Part VI:
Recommendations

Solutions to current cyber challenges exceed the capabilities and authority of any one organization alone. Moreover, cybersecurity implementation requires a layered approach across the regime complex. The following is a list of recommendations to reinforce the four ERC principles: leadership, cooperation, governance, and safeguards. These recommendations are regime complex adjuvants which can be incorporated into complexes irrespective of regime type.

People

1. *Infuse Cybersecurity into Leadership Decision-making.*

Understanding of security problems becomes more abstract the further up the decision-making chain of command. Because of information abstraction, public and private sector officials must empower cybersecurity professionals by incorporating their judgement into a broader range of organizational decisions. Private sector organizations should elevate the importance of the Chief Information Security Officer (CISO) and ensure a direct linkage to the Chief Executive Officer. Public organizations should do the same with their counterparts. At the national level, a cybersecurity must be

formalized at the Cabinet level. To this end, information exchange necessitates the development of a National Director for Information Operations (NDIO) whose position should be at the Cabinet level.

2. *Effective cooperation provides strategic peripheral vision.*

Improve unity of effort through cooperation. Improve offensive and defensive capabilities by declassifying materials and encouraging civ-mil cooperation. Legal challenges may be navigated, in some cases, through Memorandums of Understanding. If necessary, consider additional assistance from higher commands to determine whether the application of inherent powers can be utilized.[139] The ubiquitous nature of the information environment the benefits of improving strategic and operational peripheral vision outweigh the risk inherent with declassification.

3. Improve Cybersecurity Training Requirements.

Specialized training should be cyclical. Different case studies should be reviewed each cycle. Training should include practical application to ensure an understanding of the decision-making process during a potential crisis. Practical applications should also help to determine key stakeholders within an organization and identify and plan for contingencies.

Process

4. Construct Cybersecurity Policy Using Carefully Selected Language.

Carefully selected language affords better chance of adoption internationally and facilitates cooperation.

5. *Promote Cooperation Through Information Exchange: Create Nat'l Cyber Information Exchange Center.*

There is a need for interdisciplinary discussions.[140] Cooperation must widen the scope of the existing cyber strategy by strengthening partnerships with private industry through the creation of a National Cyber Information Exchange Center with the primary purposes of establishing what Lucas Kello refers to as a "Congress of Disciplines"[141] for tackling complex, uncertain, and ambiguous challenges.

6. *Consider Critical Infrastructure in Terms of Cybersecurity.*

Using the United States as an example, of the 16 critical infrastructure sectors defined by the Department of Homeland Security,[142] the Information Technology Sector is most directly related to cybersecurity. It contains important programs that require detailed integration and partnership-building. Future endeavors must reinforce existing efforts, such as Department of Homeland Security's efforts to promote a National Infrastructure Protection Plan and the Resilience Challenge to improve funding, develop understanding, and foster innovation.[143] Such efforts require effective leadership and strong partnerships committed to domestic and international information exchange.

7. *Pursue a Government Penetration Testing Program.*

To identify critical vulnerabilities and engineer potential solutions: a government penetration testing program should be pursued. First, the program should develop routine and active hacking program of government networks. Second, the program should develop routine and active hacking of military weapons systems.

8. *Improve Incentives by Funding a National 'Bug Bounty' Program.*

Establish a national 'bug-bounty' program offering recognition and/or compensation to individuals who identify software vulnerabilities and promoting transparency by incentivizing the disclosure of potential vulnerabilities.

9. Improve Understanding of Offensive Operations[144] Across the ERC.

A more clearly stated set of rules governing offensive operations is imperative. Incorporation of *Tallinn Manual 2.0: On The International Law Applicable To Cyber Operations*[145] should be considered for adoption alongside existing international laws of armed conflict to delineate the justification for capabilities such as a what constitutes active self-defense as well as the use of force and applications of digital fires.[146]

10. Improve Ability to Conduct Self-defense.

Allow non-government agencies the controlled and limited use of active cyber defensive measures outside their own boundaries. This strengthens defensive postures by providing organizations the opportunity to identify attackers and prevent future attacks. More importantly, it promotes integration and deterrence.

11. Manage Uncertainty by Developing a Set of Scenarios.

Problem framing is both backward looking and future leaning. Backward leaning refers to the use of quantitative data. Quantitative formulae are, by definition, backward looking since data can only be collected from the past and because of this quantitative data ignores novel strategies and novel threats (e.g. Panzer tanks crossing the Maginot Line could not have been predicted using available metrics at the outset of WWII).

Since risk cannot be accounted for using individual data points only, a future leaning approach must also be incorporated to describe the strategic construct. Future leaning refers to the use of a rigorously created set of strategic management scenarios to frame the universe of possible future operating environments and, using these, to develop a subset of actions across a range of events and plausible futures. Strategic scenarios offer a detailed description of a range of plausible futures and encourage the inclusion of qualitative judgement in risk and cyber governance early. Because of this, scenarios can only be used as a set and are distinct from both Courses of Action (COA) and Wargaming models. Wargaming is an event scenario and focuses on a specific future. Often, stakeholders attempt to identify the most likely COA after wargaming a specific future, but this does not fully consider the impact of world events and the ERC as whole.

Unlike COA or wargaming functions, strategic scenarios manage uncertainty by developing a subset of actions across a range of events, none of which are likely to occur, but collectively they are plausible. Although the probability of any one scenario is zero, as a set they embrace the likely range of possibilities. In contrast, if problem framing were to begin with numbers, thinking would automatically be narrowed. This is managing uncertainty.

Technology

12. Improve Response Times.

Pre-attentive processing is the subconscious ability to filter all available information and determine what is relevant. Applied to computers, use of artificial intelligence can pre-attentively process information to a degree of precision and accuracy that humans cannot. ERC stakeholders should integrate artificial intelligence to improve pre-attentive processing across environments within the ERC

where a threat can avoid human detection, or a human is too slow to react. Additionally, threat modeling created through established processes such as the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege)[147] method, will mitigate potential false alarms.

13. *Get Serious About Encryption.*

Current operational and strategic risk analysis fails to accurately assess the benefits of encryption as a form of risk mitigation. Superimposing Moore's law, which suggests the number of transistors per square inch doubles every year, the more integrated the environment, the more ubiquitous the potential threat.[148] Cryptographic tools such as the use of cryptographic keys provide enhanced privacy and security. Software systems designed to promote system processes which require operating systems to accept cryptographic keys, for example, is one way to mitigate potential threats. More important, though, is the implementation of cryptography incorporated as part of a larger security strategy. Current applied cryptographic technologies are as much as 40 years old.[149] ERC stakeholders must ensure implementation of the most up to date encryption.

14. Implement Performance Based Metrics & Exchange Results.

Like-minded nation states and engaged stakeholders should conduct periodic fire-drills to ensure that established international and technical standards are being implemented. Periodic screening of assets should be incorporated to detect and deter insider threats. These screenings should equate to periodic drug testing. Additional metrics should include pre-attentive processing diagnostics. Consider tying productivity to proposed planning and operations improvements to determine additional unforeseen costs and/or benefits.

15. Integrate and Expand Cybersecurity-Related Research and Development.

Integrate research and development projects to the maximum extent practicable. Increase cybersecurity-related funding. Incentivize cybersecurity-related research through tax incentives and federal grants.

16. Integrate Cloud Computing.

Cloud computing is an excellent example of the confluence of people, process, and technology and will be examined in detail to break out the respective components pertinent to each.

Cloud computing is growing at a rate 4.5 times faster than the rate of IT spending, a difference which is projected to widen further as the migration of data storage to cloud-based storage continues to grow.[150] Although the U.S. government recognizes the value of cloud computing, federal agencies are slow to transition to cloud-based solutions. While many private sector companies have long-embraced cloud computing in pursuit of better value, the government has been more reluctant to migrate to cloud-based computing due to concerns over downtime, security, and overall control of the data.

Despite these concerns, however, federal agencies are increasingly adopting cloud-based solutions. According to the research firm Govini, which studies infrastructure modernization and cloud market growth, the U.S. government spent $3.3 billion on cloud computing in fiscal year 2015. Much of this growth originated from the 2011 *Cloud First Policy*, released by the Obama administration. Recognizing the potential benefits of cloud computing the policy mandated government agencies to evaluate cloud computing options prior to financing any new investments.[151]

The policy identified three main sources of value that cloud-based solutions can provide: efficiency, agility, and innovation. First, efficiency is gained by the cloud's ability to maximize use of available resources using advanced tools which automate former tasks such as systems administration. The integration of automated technologies results in substantial cost savings, more reliable IT

infrastructure, and increasingly simplified IT management. Additional efficiency is possible by prioritizing the migration of high cost low demand services to the cloud over services which are less expensive to maintain.[152]

Second, cloud computing improves agility by allowing agencies to rapidly scale up or down services as required to meet unpredictable demand. Agility in cloud computing also reduces the need rely on IT investments based on forecasts, which are often challenged by unforeseen events.[153]

Finally, the *Cloud First Policy* identifies cloud computing as an enabler of innovation. Cloud computing reduces the cost and timing of project development, operational testing, and evaluation which results in lower investment costs and reduced risk.[154] Lower costs at reduced risk foster experimentation. For example, cloud computing provides an opportunity to leverage automation in ways not previously possible due to the ability to experiment with automation at scale.

Despite significant investment, resulting from government agency evaluations of cloud computing required by the *Cloud First Policy,* government spending has recently stalled out. In fact, a report published by International Data Corporation (IDC) revealed federal spending on cloud-based solutions are set to drop in 2017 $2.2 billion.[155] In contrast, global investment in cloud-based systems has continued to grow. According to *Forbes* magazine, investment was projected to attain $246 billion in 2017, up from $209 billion in 2016.[156]

Three factors have led to the government's slowed progress: concerns over downtime, control, and security. Downtime and control, were addressed early on by many government agencies resulting from initial cloud assessments. Rather than relying on public based cloud systems, government agencies employing cloud-based services developed private cloud networks. These private cloud networks offered the benefits of agility and were also assessed to be more reliable in handling certain workloads required by these agencies.[157] By implementing private cloud infrastructure, early adopters quickly addressed concerns over downtime while retaining overall control of their data. Unfortunately, in

contrast to a public cloud or even a hybrid solution, the benefits of lost cost were not fully realized. Simply migrating to a public cloud is not an option for many government organizations however, mainly due to security rationale.

Finally, the U.S. government must address security concerns and federal regulations many private organizations do not. Advanced persistent threats require routine security-wide system updates.[158] The short duration between system updates are uniquely challenging, which many government organizations have yet to solve.

Additionally, federal regulations related to data security on cloud-based systems slows migration further. For example, vendors who desire to service the DOD with cloud-based services must ensure a minimum of Information Impact Level 5. Impact Level 5 requires handling of controlled unclassified information, or CUI, which includes information classified as personally identifiable information (PII) and protected health information (PHI)[159]. Vendors seeking government contracts must also ensure Impact Level 5 information is physically separated between DOD and non-DOD customers. In Jan 2017, Microsoft became the first company to achieve DoD's newest iteration of standards.[160] Since then, other companies have achieved Impact Level 5 security standards as well. While the process has undoubtedly been caused cloud-migration to slow, vendors are catching up. In September, for example, Amazon Web Services earned the DoD provisional authorization to handle high capacity, mission-critical workloads required of DoD systems to include the newest version of the DoD's global positioning system (GPS) satellites.[161] So far, the results have been beneficial for both vendors and the government. Coupled with the use of automation and a defense in depth strategy to include zero trust verification, cloud-based solutions are not only lower cost, but increasingly more secure. For example, AWS integration with the U.S. Air Force GPS systems resulted in a 30 percent savings in overall storage costs and considered secure enough to play a significant role in a U.S. strategic asset.[162]

Despite U.S. government efforts to incorporate cloud-based solutions, slow progress has been made in migrating over to cloud-based solutions resulting from various concerns pertaining to downtime, security, and overall control of the data. Government agencies, however, continue to assess the benefits over the cloud relative to the risks. As solutions are developed to alleviate these concerns, government agencies will progressively continue to move from a model where users and applications operate inside a trusted network to a model where users and applications exist everywhere, and no one is trusted until verified.

Conclusion

Cybersecurity challenges are manifold. Vulnerabilities, left unaddressed, create unnecessary risk to global security. The ubiquitous information environment requires a mental construct capable of addressing challenges to appropriate stakeholders. Therefore, a whole of society approach to enhanced understanding and improving decision-making is necessary to respond to actions within a complex, uncertain, and ambiguous environment. Rogue conduct within the ERC must be met with effective leadership, extensive stakeholder engagement, sound governance, and practical safeguards to facilitate the effects of adjuvant security across the ERC and provide strategic inoculation against future cyber-borne threats. Because there is no single 'cure' for all existing cyber challenges within the ERC, adjuvant security must be applied.

Endnotes

[1] Centers for Disease Control and Prevention, *Vaccine Adjuvants,* Updated on September 12, 2016, https://www.cdc.gov/vaccinesafety/concerns/adjuvants.html.
[2] Centers for Disease Control and Prevention, *Vaccine Adjuvants.*
[3] Note: The formulation of the Enhanced Regime Complex owes itself to the extensive work completed by Joseph S. Nye, Jr., from his paper "*The Regime Complex for Managing Global Cyber Activities*," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014). This paper is an attempt to preserve those concepts while providing a new perspective to existing challenges.
[4] Ibid; Nye, p.5.
[5] Stephen Krashner, ed., "*International Regimes*," (Ithaca, NY: Cornell University Press, 1983), quoted in Joseph S. Nye, Jr., "*The Regime Complex for Managing Global Cyber Activities*," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014), p.5.
[6] Ibid; Nye, p.11.
[7] Ibid; Nye; p.5.
[8] Ibid; Nye, p.13.
[9] Ibid; Nye, p.7.
[10] Ibid; Nye, p.9.
[11] Clausewitz, Carl Von, *On War*, trans. Michael Howard, and Peter Paret (Princeton: Princeton University Press, 1984), pg.366.
[12] Clausewitz; p.482. ("A defensive action ought to be a slow, persistent, calculated business, entailing definite risk.")
[13] Clausewitz; p.379. ("Waiting…the main feature of defense and also its chief advantage.")
[14] Clausewitz; p.357. ("What is the concept of defense? The parrying of a blow. What is the characteristic feature? Awaiting the blow…What is the object of defense? Preservation.")
[15] Clausewitz; p.370 ("A sudden powerful transition to the offensive – the flashing sword of vengeance – is the greatest moment for the defense.")
[16] Clausewitz; p.358 ("We have already indicated in general terms that defense is easier than attack. But defense has a passive purpose: preservation; and attack a positive one: conquest. The latter increases one's capacity to wage war; the former does not.")
[17] Thucydides, Edited by Strassler, Robert B., *The Landmark Thucydides: A Comprehensive Guide To The Peloponnesian War*, (New York: Free Press, 1996), Book 7, 7.73, p.430.
[18] Federal Communications Commission, "Cyber Security Planning Guide: Small Biz Planning Guide," (Washington D.C.: 2012), PDS-5.
[19] Clausewitz; p.93.
[20] Warwick Ashford, "Cyber Attacks Not Impossible to Manage, Says ex-GCHQ Head," *ComputerWeekly*, November 9, 2017, (TechTarget), http://www.computerweekly.com/news/450429790/Cyber-attacks-not-impossible-to-manage-says-ex-GCHQ-head, p1.
[21] Ashford; p1.
[22] Telis Demos, "Banks Build Line of Defense for Doomsday Cyberattack," *Wall Street Journal*, December 3, 2017, https://www.wsj.com/article_email/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401-lMyQjAxMTA3NjA0NDUwODQxWj/.
[23] Deborah Plunkett and Harrison Monsky, "The Cybersecurity Campaign Playbook," *Defending Digital Democracy*, November 20, 2017, Version 1.3, Harvard Kennedy School, Belfour Center for Science and International Affairs, p7.
[24] Ashford; p2.
[25] Federal Communications Commission, "Cyber Security Planning Guide: Small Biz Planning Guide," (Washington D.C.: 2012), EMP-1.
[26] Plunkett and Monsky; p5.

[27] Plunkett and Monsky; p11.
[28] Federal Communications Commission, "Cyber Security Planning Guide: Small Biz Planning Guide," (Washington D.C.: 2012), PDS-5.
[29] Federal Communications Commission; IR-1.
[30] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Ver. 1.0, February 12, 2014, https://www.nist.gov/cyberframework, p.8.
[31] Armor, "Of #@$%! I've Been Breached: what To Do Next," *Armor*, http://cs.brown.edu/people/jes/EMCS2600Readings/Module5/2017_ARMOR_Whitepaper_Surviving_A_Breach.pdf, p.3.
[32] Mara Hvistendahl, "Inside China's Vast New Experiment In Social Ranking," *Wired*, December 14, 2017, https://www.wired.com/story/age-of-social-credit/.
[33] Clausewitz; p.370 ("A sudden powerful transition to the offensive – the flashing sword of vengeance – is the greatest moment for the defense.")
[34] Clausewitz; p.357. ("Pure defense, however, would be completely contrary to the idea of war, since it would mean that only one side was waging it.")
[35] Peter Cooper, "Cognitive Active Cyber Defense: Finding Value Through Hacking Human Nature," *Journal of Law and Cyber Warfare*, Winter 2017, Vol.5, No. 2, http://cs.brown.edu/people/jes/EMCS2600Readings/Module1/2017_JLCW_5_2_CognitiveActiveCyberDefense_Cooper.pdf, p.63.
[36] US DoD, *Department of Defense Dictionary of Military and Associated Terms*, 2001 US DEP. DEF. JT. PUBL. 1–513 (2015).
[37] Cooper; p.63.
[38] Sharon Thiruchelvam, "Lies and chatbots are also undermining commerce," *Raconteur*, December 17, 2017, http://cs.brown.edu/people/jes/EMCS2600Readings/Module6/2017_12_17_Raconteur_LiesAndChatbotsAreAlsoUnderminingCommerce.pdf.
[39] Michael I. Handel, *Masters Of War: Classical Strategic Thought*, 3d Ed., (Frank Cass: London, 2005), p.355.
[40] Thiruchelvam.
[41] Mao Tse-Tung, Selected Works of Mao Tse-Tung, Vol.2, (Pergamon: Oxford, England, 1965), p.143.
[42] Michael Levin, "Five Steps Users Can Take To Inoculate Themselves Against Fake News," *Center For Information Security Awareness*, Published March 06, 2017, Updated April 04, 2017, p.2-3.
[43] Plunkett and Monsky; p.7.
[44] Louis Pasteur, Lecture, University of Lille, December 7, 1854, referenced by Dr Jerry Krause in "Chance Favors The Prepared Mind", P*rincipia-Scientific,* December 20, 2017; (The actual quote is "*Dans les champs de l'observation le hasard ne favorise que les esprits préparés.").*
[45] Cooper; p.57.
[46] Clausewitz; p.372.
[47] Note: For more on cyberspace as a substrate refer to Part V: Challenges, p.33-34.
[48] Joint Publication 3-12 R, *Cyberspace Operations*, February 5, 2013, (Washington, D.C.), p.v-vi.
[49] Daniel T. Kuehl, "*From Cyberspace to Cyberpower: Defining the Problem,*" In *Cyberpower and National Security,* ed.'s Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (Washington, D.C.: National Defense University Press), p.26, quoted by Joseph S. Nye, Jr., "*The Regime Complex for Managing Global Cyber Activities*," Global Commission on Internet Governance, Center for International Governance Innovation and the Royal Institute for International Affairs, (Chatham House: May 2014), p5.
[50] Aven and Renn (2009) and SRA Glossary (2015); International Risk Governance Council (IRGC); p.5.
[51] Lucas Kello, *The Virtual Weapon and International Order,* (Yale, 2017), p.29, quoted in Kristen Eichensehr, "Today's Revolution: Cybersecurity and the International Order," *Lawfare*, January 8, 2018, https://lawfareblog.com/todays-revolution-cybersecurity-and-international-order, p.1.
[52] Clausewitz, Carl Von, *On War*, trans. Michael Howard, and Peter Paret (Princeton: Princeton University Press, 1984), pg.366.
[53] Ibid; Obama, Barack H., *National Security Strategy,* Foreward.
[54] The White House. Foreign Policy. *Cybersecurity – Executive Order 13636*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[55] Lewis, Ted G., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, (Somerset, US: John Wiley & Sons, Incorporated, 2014), ProQuest ebrary, Published 2014, p164.
[56] Kristen Eichensehr, "Today's Revolution: Cybersecurity and the International Order," *Lawfare*, January 8, 2018, https://lawfareblog.com/todays-revolution-cybersecurity-and-international-order, p.3.
[57] Ibid; Eichensehr, p.3.
[58] The White House, Foreign Policy, *Cybersecurity – Executive Order 13636*.
[59] Ibid; Eichensehr, (referencing Lucas Kello, *The Virtual Weapon and International Order, p7.),* p.1.
[60] Gardete, Pedro M., *"Incentives to Share Market Information: the Case of the Dynamic Random-Access Memory Industry,"* Stanford University, May 2013, p29, http://www.economics.cornell.edu/sites/default/files/files/events/Pedro.Gardete.pap_.pdf.
[61] Joint Publication 3-12, IV-8.
[62] Milan N. Vego, *Joint Operational Warfare, Theory And Practice,* rep of 1st ed., (Newport, R.I.: U.S. Naval War College; 2009), VIII-15.
[63] Vego; VIII-15.
[64] Vego; VIII-15.
[65] LtCol Parker Wright, USAF, *Digital* Theaters, Decentralizing Cyber Command and *Control,* Published April 2014, Center for a New American Security, 8-10.
[66] Ellen Nakashima, *The Washington Post*, "U.S. military cyber operation to attack ISI last year sparked heated debate over alerting allies," Published May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.999b5198e735.
[67] International Risk Governance Center, *"Introduction to the IRGC Risk Governance Framework,"* revised version 2017, (Lausanne: EPFL International Risk Governance Center), pg.5.
[68] Ibid; IRGC, p.5.
[69] John Lark, "ISO 31000: Risk Management, A Practical Guide for SMEs," referencing ISO 31000: 2009, Clause 2.1, (Geneva, Switzerland, 2015), p.13.
[70] Ibid; International Risk Governance Center, "Introduction to the IRGC Risk Governance Framework," referencing Aven and Renn (2009) and SRA Glossary (2015); p.5.
[71] Ibid; IRGC; p.5.
[72] Ibid; IRGC, p.10.
[73] LtCol Jeffrey N. Rule, USMC, *"A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought,"* US Army War College, 2013, www.dtic.mil/dtic/tr/fulltext/u2/a590672.pdf, p.9.
[74] Ibid; Nye, p.6.
[75] Ibid; Eichensehr, p.2.
[76] Ibid; Eichensehr, p.2.
[77] Obama, Barack H. Federal Register. Vol.78. No.33. Presidential Documents. *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*. February 12, 2013. Accessed on October 29, 2016. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[78] Ibid; Nye, p.6.
[79] Lewis, Ted G., *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, (Somerset, US: John Wiley & Sons, Incorporated, 2014), ProQuest ebrary, Published 2014, p172.
[80] https://www.gpo.gov/fdsys/pkg/CPRT-112HPRT67344/pdf/CPRT-112HPRT67344.pdf
[81] The White House, Press Office, *Presidential Memoranda,* Accessed on February 16, 2018, https://www.whitehouse.gov/briefing-room/presidential-actions/presidential-memoranda.
[82] 114 Stat. 2763A-154 Public Law 106-554, Appendix C, 106th Congress, Approved 21 December 2000, Accessed 7 March 2017, https://www.gpo.gov/fdsys/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf
[83] "*The National Strategy to Secure Cyberspace*," Published February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, p.30.
[84] B.J. Heiman, "*Cybersecurity Regulation is Here!*," 12th Annual RSA Security Conference, Published on 15 April 2003, http://www.klgates.com/files/Publication/b107a7ae-1e01-404e-830d-5f4a20eebd1b/Presentation/PublicationAttachment/dbb0ff0d-33fd-4808-b338-60b3345450f6/CybersecurityRegisHere.pdf.

[85] Jason Healey, "*A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,"* (CCSA Publication: In Partnership with the Atlantic Council, 2013), p15.
[86] Ibid; Healey.
[87] AT&T, "*Submarine Cables: Critical Infrastructure, Cable Owner's Perspective,*" Published on 20-21 May 2017, http://www.virginia.edu/colp/pdf/Wargo-presentation.pdf, p.3.
[88] Ibid; AT&T, p.2.
[89] Allan Friedman and P.W. Singer, "*Cybersecurity And Cyberwar: What Everyone Needs To Know,"* (New York: Oxford University Press, 2014), p167.
[90] Brett T. Williams, *"The Joint Force Commander's Guide to Cyberspace Operations,"* National Defense University Press, Joint Force Quarterly 73, April 01, 2014, http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/.
[91] U.S. Department Of State*, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 1967, https://www.state.gov/t/isn/5181.htm.
[92] Note: "War v. Armed Conflict. Historically, the applicability of the LOAC often depended upon a State subjectively classifying a conflict as a "war." Recognition of a state of war is no longer required to trigger the LOAC. After the 1949 Geneva Conventions, the LOAC is now triggered by the existence of "armed conflict" between States. "The substitution of [armed conflict] for the word 'war' was deliberate." (Ibid; p7).
[93] International and Operational Law Department, *"Law Of Armed Conflict Deskbook,"* Judge Advocate General's Legal Center, Charlottesville, VA, 2012, https://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf, p143.
[94] Schmitt, Mike, *"Tallinn 2.0: On The International Law Applicable To Cyber Operations,"* (Cambridge: Cambridge University Press, 2017), p452.
[95] Michael Schmitt, "Rules of Engagement: Factors and Analysis," Lecture, April 2017, U.S. Naval War College (with permission from author).
[96] Rep. Tom Graves (R-GA-14), Active Cyber Defense Certainty Act: Bipartisan Bill Empowers Americans to Develop New Defenses Against Cyber Attacks," October 13, 2017, (Washington, D.C.), http://cs.brown.edu/people/jes/EMCS2600Readings/Module8/acdc_expaliner.pdf.
[97] Chris Demchak, lecture on March 16, 2017, "*Complexity, Cybered Conflict, and Socio-Technical Systems' Surprise*," U.S. Naval War College.
[98] NSA, *Information Assurance Directorate: NSA Methodologies for Adversary Obstruction*, Published August 2015, https://www.iad.gov/iad/library/reports/nsa-methodology-for-adversary-obstruction.cfm.
[99] Capt. Wayne P. Hughes, Jr., *Fleet Tactics and Costal Combat*, (Annapolis, M.D.: U.S. Naval Institute: 2000), 25.
[100] Joint Publication 3-12, II-1.
[101] Joint Publication 3-12, GL-4.
[102] Chris C. Demchak, lecture on March 16, 2017, *Complexity, Cybered Conflict, and Socio-Technical Systems' Surprise*, U.S. Naval War College.
[103] Chris C. Demchak and Peter Dombrowski, *Rise of a Cybered Westphalian Age*, Strategic Studies Quarterly, Spring 2011, p35.
[104] Ibid; Nye, p.5.
[105] Antoine-Henri Jomini, *The Art of War*, trans. Capt. G.H. Mendell and Lieut. W.P. Craighill (Rockville, MD: Arc Manor, 2007), 29.
[106] Joint Publication, 3-12, I-3.
[107] Department of the Army, *Field Manual 3-12: Cyberspace And Electronic Warfare Operations*, (Washington, D.C., April 17, 2017), 2-3.
[108] S.A. Helm, CYBER FLAG 15-1 Trip Report (Unclassified: U.S. Naval War College, 26 November 2015).
[109] Kim Zetter, "An Unprecedented Look At Stuxnet, The World's First Digital Weapon," *Wired*, November 3, 2014, excerpted from Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Penguin Random House, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[110] Robert Kozloski, "The Information Domain as an Element of National Power," *Center for Contemporary Conflict*, December 2008, p.1. https://www.hsdl.org/?view&did=232244,
(Note: "The DoD defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.").

[111] Louis P. Pojman, Peter Tramel, ed., "Part III: Ethics and Egoism," *Moral Philosophy: A Reader,* 4th Ed., (Indianapolis: Hackett Publishing, 2009), https://books.google.com/books?id=ugU7BAAAQBAJ&pg=PA60#v=onepage&q&f=false, p.60.
[112] Adam Smith, An Inquiry Into The Nature And Causes Of The Wealth of Nations, (Apollis Publishing: E-reader), https://read.amazon.com/?asin=B078YSWTHB, p.279, ("In the absence of enthusiasm and of an ardent faith, great sacrifices may be obtained from the members of a commonwealth by an appeal to their understandings and their experience; each individual will feel the same necessity for uniting with his fellow-citizens to protect his own weakness; and as he knows that if they are to assist he must co-operate, he will readily perceive that his personal interest is identified with the interest of the community.").
[113] Alexis de Tocqueville, Democracy In America, Henry Reeve, trans., Vol 1, Bk 1, Intro, p.19, ("In the absence of enthusiasm and of an ardent faith, great sacrifices may be obtained from the members of a commonwealth by an appeal to their understandings and their experience; each individual will feel the same necessity for uniting with his fellow-citizens to protect his own weakness; and as he knows that if they are to assist he must co-operate, he will readily perceive that his
personal interest is identified with the interest of the community.").
[114] *The Economist*, "Profit and the public good: Companies that merely compete and prosper make society better off," January 20, 2005, http://www.economist.com/node/3555259.
[115] Benjamin Franklin (attributed to), "Poor Richard, 1741," *National Archives*, (Note: This quote is generally attributed to Benjamin Franklin, although his actual words differed somewhat in written form: "he is ill clothed that bare virtue," adding that "a good conscience is a continual Christmas"), https://founders.archives.gov/documents/Franklin/01-02-02-0066.
[116] James Madison, "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments," *Independent Journal*, February 6, 1788, (Federalist Paper #51), http://www.constitution.org/fed/federa51.htm, ("If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.").
[117] Lee Drutman and Steven Teles, "Why Congress Relies on Lobbyists Instead of Thinking for Itself," *The Atlantic*, March 10, 2015, http://cs.brown.edu/people/jes/EMCS2600Readings/Module7/2015_03_10_TheAtlantic_CongressionalReformShouldStartWithProfessionalStaff.pdf.
[118] James Madison, "The Same Subject Continued: The Union as a Safeguard Against Domestic Faction and Insurrection," *The New York Packet*, November 23, 1787, (Federalist Paper #10), https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-10. ("There are again two methods of removing the causes of faction: the one, by destroying the liberty which is essential to its existence; the other, by giving to every citizen the same opinions, the same passions, and the same interests…By what means is this object attainable? Evidently by one of two only. Either the existence of the same passion or interest in a majority at the same time must be prevented, or the majority, having such coexistent passion or interest, must be rendered, by their number and local situation, unable to concert and carry into effect schemes of oppression.").
[119] Derek B. Johnson, "House Dem revives data breach bill after Equifax hack," *FCW*, September 18, 2017, http://cs.brown.edu/people/jes/EMCS2600Readings/Module7/2017_09_18_FCW_HouseDemrevivesDataBreachBillAfterEquifaxHack.pdf.
[120] Pam Greenburg, "Security Breach Notification Laws," *National Conference of State Legislatures*, April 12, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[121] Ibid; Johnson.
[122] Department of Homeland Security, "Information Sharing," *DHS*, Published September 27, 2016, https://www.dhs.gov/topic/cybersecurity-information-sharing.
[123] Brietta Hague, "'Every Country Should Have a Cyber War': What Estonia Learned from Russian Hacking," *Defense One*, August 16, 2017, http://cs.brown.edu/people/jes/EMCS2600Readings/Module7/2017_08_14_DefenseOne_WhatEstoniaLearnedFromRussianHacking.pdf.

[124] Ibid; Hague.
[125] De Tocqueville; p.596.
[126] Vego; I-6
[127] Information Technology Labs at the National Institute for Standards & Technology, *Best Practices*, Updated March 9, 2017, Accessed 19 August 2017, https://www.nist.gov/topics/best-practices.
[128] Admiral Michael Mullen, preface to Joint Publication 5-0: Joint Operational Planning, (Washington, D.C., August 11, 2011), http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.
[129] Joint Publication 3-12, x.
[130] Joint Publication 3-12, xii.
[131] Department of Defense, Information Security Program: Overview, Classification, and Declassification, (Washington, D.C., February 24, 2012), Encl 2, 18, http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf.
[132] Michael T. Goodrich and Roberto Tamassia, *Introduction to Computer Security,* (Boston: Pearson Education, 2011), 3.
[133] Goodrich, Michael T. and Tamassia, Roberto. *Introduction to Computer Security.* (Boston: Pearson Education, 2011). Cr 1, 4.
[134] Goodrich, Michael T. and Tamassia, Roberto. Ch 1, 6.
[135] Goodrich, Michael T. and Tamassia, Roberto. Ch 1, 8.
[136] Bernardo Palazzi, interview with author, May 8, 2017.
[137] Jerome Saltzer and Michael Schroeder, The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 1975, 63(9): 1278-1308.
[138] Adam Shostack, *Threat Modeling: Designing for Security,* (Indianapolis: John Wiley & Sons, 2014). Pg.61
[139] Library Of Congress, *Presidential* Powers, Updated June 9, 2015, Accessed on 10 August 2017, https://www.loc.gov/law/help/usconlaw/pres-powers.php.
[140] Kristen Eichensehr, "Today's Revolution: Cybersecurity and the International Order," *Lawfare*, January 8, 2018, https://lawfareblog.com/todays-revolution-cybersecurity-and-international-order, p.3.
[141] Lucas Kello, *The Virtual Weapon and International Order,* (Yale, 2017), p.29, quoted in Kristen Eichensehr, "Today's Revolution: Cybersecurity and the International Order," *Lawfare*, January 8, 2018, https://lawfareblog.com/todays-revolution-cybersecurity-and-international-order, p.3.
[142] Department of Homeland Security. *Critical Infrastructure Sectors*, https://www.dhs.gov/critical-infrastructure-sectors.
[143] Department of Homeland Security. *National Infrastructure Protection Plan*, https://www.dhs.gov/national-infrastructure-protection-plan.
[144] Note: Offensive capability warrants discussion at the unclassified level. While discussion of offensive operations should maintain a higher classification, mention of offensive capabilities is beneficial because it conveys acknowledgement and provides for the ability to determine, through policy, what distinguishes offensive from defensive operations.
[145] Schmitt, Michael E., Ed., Vihul, Liis, Ed. *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. (Cambridge: Cambridge University Press, 2017).
[146] Joint Fires Support. Joint Publication 3-09. III-4. http://dtic.mil/doctrine/new_pubs/jp3_09.pdf.
[147] Shostack, Adam, *Threat Modeling: Designing for Security*, (Indianapolis: John Wiley & Sons, 2014), p.61.
[148] Michael Perrottet, "Connected Vehicle Technology and Privacy", EMCS 2010, Module 7, 17 June 2017.
[149] Anna Lysyanskaya, "Authorized, But Anonymous: Taking Charge of Your Personal Data", Brown University, EMCS Keynote Speech, 01 October 2017.
[150] Louis Columbus, "Roundup Of Cloud Computing Forecasts, 2017, *Forbes,* 29 April 2017, https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#1f2f4f3a31e8.
[151] Vivek Kundra, "Federal Cloud Computing Strategy", *The White House,* 8 February 2011, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf, p2.
[152] Ibid; Kundra, p7.
[153] Ibid; Kundra, p8.
[154] Ibid; Kundra, p9.

[155] Shawn McCarthy, "U.S. Federal Government Cloud Forecast, 2017-2021", *IDC,* April 2017, https://www.idc.com/getdoc.jsp?containerId=US41803117.
[156] Ibid; Columbus.
[157] Sujatha Perepa, "Why The U.S. Government Is Moving To Cloud Computing", *Wired,* September 2013, https://www.wired.com/insights/2013/09/why-the-u-s-government-is-moving-to-cloud-computing/.
[158] Joshua Bleigerg and Darrell M. West, "Analyzing the Federal Government's Use of the Cloud", *Brookings,* 9 February, 2015, https://www.brookings.edu/blog/techtank/2015/02/09/analyzing-the-federal-governments-use-of-the-cloud/.
[159] Information Assurance Support Environment (IASE), "Information Security Objectives/Impact Levels", *Defense Information Systems Agency (DISA)* , 23 January 2015, https://iase.disa.mil/cloud_security/cloudsrg/Pages/ImpactLevels.aspx.
[160] Frank Konkel, "Microsoft Gets Big Cloud Win in Defense Department", *Nextgov,* 18 January 2017, http://www.nextgov.com/it-modernization/2017/01/microsoft-gets-big-cloud-win-defense-department/134670/.
[161] Chris Gille, "AWS Earns Department of Defense Impact Level 5 Provisional Authorization", *Amazon,* 12 Sep 2017, https://aws.amazon.com/blogs/security/tag/impact-level-5/.
[162] Ibid, Gille.