Penn State Journal of Law & International Affairs

Volume 5
Issue 1 *War in the 21st Century and Collected Works*

April 2017

A Research Agenda to Improve Decision Making in Cyber Security Policy

Benjamin Dean

Rose McDermott

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2017 VOLUME 5 NO. 1

A RESEARCH AGENDA TO IMPROVE DECISION MAKING IN CYBER SECURITY POLICY

Benjamin Dean and Rose McDermott

TABLE OF CONTENTS

I. SECTION 1

A. Introduction

A lot of recent media attention and an enormous amount of taxpayer dollars have been focused on issues surrounding cyber security. Problems arise because many people mean many different things in referring to cyber security, and different groups have different, often conflicting or even mutually contradictory goals, in pursuing such policy. Some companies and users privilege security; the government places a premium on surveillance, and users vary in their concerns regarding privacy, often not fully understanding the relationship between personal and technical aspects of the term.

Much of the debate around cyber security has generated more heat than light, especially in the wake of the Snowden revelations, often because those who know a lot about the technical aspects of cyber issue know little and care less about government concerns, while those in the policy arena are often willfully unaware of the technical aspects of the domain they are expected to regulate. Everyone can agree that no one wants a foreign country to infiltrate their infrastructure or compromise their financial, transportation, medical, utility or nuclear weapons systems. And everyone agrees that cyber-crime and exploitation are common problems that need to be addressed. But very few know how to go about it.

Many of the discussions around cyber security seem to go around in circles with very little forward progress, in part because the decision-making that generates such policy remains poorly informed and systemically hindered. Here we hope to begin to improve decision-making by providing a theoretical rubric for understanding the underlying factors that influence decision-making across different levels and fields of discipline. In addition, we hope to highlight some of the inherent difficulties in developing successful policy within each step and between areas of inquiry. We then offer a research agenda to guide research into improving decision-making going forward.

1. *Levels of Analysis.*

By the term 'cyber security policy', we refer to policy interventions that coordinate and direct resources toward improving cyber security. Improving cyber security involves protecting computer networks and systems and the users of these technologies (including people and organizations) against physical and financial loss. Decision-making contributes to the formulation of policy interventions at four levels: international, national, organizational, and individual.

Interventions differ across levels. For instance, treaties or agreements are used at the international level, laws and regulation at the national level, and internal policies or codes of conduct at the organizational level.

[Table 1 on following page]

Table 1: A conceptual framework for cyber security policy decision-making

Level	Entities	Factors influencing decision making	Common policy interventions
International	Nation state, international fora and organizations	Lack of institutional structure for non-state actors Diffusion of power No enforcement mechanism Rigidity	Agreements Treaties
National	National government, legislative or executive branch	No national strategy Dispersed responsibility	Law Regulation
Organizational	Private enterprise or governmental administrative agency	Lack of evidence base Rigidity Lack of technical knowledge Lack of coordination and communication between technical experts and policymakers	Company policy Code of conduct Contracts
Individual	Individual person	Loss aversion Uncertainty/information asymmetry	Heuristics Hacker culture Decision making norms

At an international level, the system for mediating relations between nation states is not built in a way that allows for inclusion of non-state actors, which are inherent to any issue connected to digital technologies and the Internet. This, coupled with the dispersion of power among states, individuals and non-state actors, makes enforcement of international treaties or agreements difficult, even if they are agreed upon and enacted.

At a national level, the lack of national strategy and dispersed responsibilities for cyber security policy lead to contradictory policy proposals and unintended consequences that ultimately reduce overall cyber security. There is often a lack of communication and integration between the public and private sector, both of which operate in this space simultaneously. In addition, governments and technology firms may have entirely antagonistic goals in certain areas, including those involving privacy, security and surveillance, as the confrontation between the FBI and Apple over unlocking the San Bernadino shooter's iPhone so richly illustrates.

At an organizational level, deficiencies in the information or evidence base with which to make decisions mean that 'good' programs are not identified and 'bad' ones are not eliminated. This problem is coupled with, and compounded by, a chronic lack of technical knowledge in those organizations with responsibility to respond to cyber security matters, and a simultaneous lack of understanding of policy needs and processes within the technical community.

At an individual level, loss aversion in a situation that is inherently uncertain systematically restricts optimal decision making by encouraging individual leaders to revert to automatic and natural psychological strategies and procedures in decision-making. These strategies and procedures may not be well suited for the complex problems or challenges they confront. Risk can be mitigated through processes, such as insurance, in ways that uncertainty cannot. Uncertainty tends to make people more cautious, especially in the wake of potential catastrophic failure; this puts defenders at a disadvantage relative to attackers.

The decision-making by entities at each of these four levels are influenced by various factors, not all of which work in the same direction. Various incentives and disincentives, constraints and heuristics or biases influence the way in which policy mechanisms are developed, or the ways in which people behave in response to policy interventions. Some of these factors are unique to one level and some apply to many (e.g. lack of information, rigidity, dispersed power).

It is our contention that the development and deployment of policy interventions are influenced by various institutional, organizational, human psychological and behavioral, economic and political biases or heuristics. These influences become encoded in the decision-making mechanisms themselves, which in turn, push those who are subject to the interventions to behave or react in ways that mirror the biases or heuristics or the designers of the interventions themselves.

The cyber security field is in constant flux, and issues related to decision-making are inherently multidisciplinary, which necessitates timely, ongoing and integrated research to keep our societies as productive and secure as possible. In listing the factors that influence decision-making, we draw on the disciplines of international relations, economics, organizational behavior, cognitive and behavioral sciences, psychology and public policy.

How then can we make better decisions in cyber security policy? Section one provides an overview of the obstacles to effective decision-making in cyber security policy at the international, national, organizational and individual levels. A number of interventions might be instituted to try to begin to overcome the various factors that negatively influence decision-making in cyber security policy. In the third section, we propose some specific examples linked to the systemic factors we identify as influencing decision-making in section two. The last section offers a research agenda designed to support the development of the proposed interventions we discuss in section 3.

II. SECTION 2

This section provides an overview of the obstacles to more coherent and coordinated cyber security policy across levels (international, national, organizational and individual) by discussing issues within each level, describing what has been done in the past and in some cases describing the past limitations to success.

A. International

1. *Lack of Institutional Architecture to Deal with Non-State Actors.*

Within international relations theory, the realist school of thought characterizes the international system as anarchic. It is one in which individual states each act in their own self-interest, unable to cooperate out of mistrust of one other. The international system is one comprising Westphalian nation states. This model has prevailed since the treaty for which the system owes its name in 1648. The liberal school of international relations theory called for the creation of a set of international organizations and norms to manage the relations between states in this otherwise anarchic international system.

The Internet, as a network of networks, is not bound strictly by national boundaries in law or in practice, since communication across borders in this system is constant. Cyber-security thus presents a problem that an international system comprised of nation states is ill equipped to solve. So-called 'non-state' actors fill the ecology of cyber-security, from private companies that develop the software and hardware, private Internet service providers, organized criminal outlets and individual 'hackers', not to mention both business and personal users of the Internet. While there is some interaction between state and non-state entities, such as relationships between Russian law enforcement and intelligence agencies with organized criminal groups,[1] and between the Chinese military and semi-autonomous hacking groups, these non-state interests are not present

[1] *See* BRIAN KREBS, SPAM NATION (Sourcebooks, Inc., 2014).

within the delegations representing the respective nation states in international organizations and fora.

A patchwork of international agreements and treaties are linked to cyber-security.[2] One multilateral agreement, drafted under the aegis of the Council of Europe, is The Budapest Convention on Cyber Crime. Signed in 2001, it is open to non-European signatories and has the objective of pursuing, "a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."[3] The Budapest Convention has attracted 50 signatories. However, it is still criticized as being outdated and has not gained the support of key countries in cyber security such as Brazil and Russia.[4]

On a bilateral level, a number of recent agreements have been created with the intention of curbing cyber-espionage between the United States and China,[5] between China and the United Kingdom,[6] China and Germany[7] and between China and Russia.[8] Questions have been raised as to whether or not the bilateral agreements, particularly

[2] *See* Jonathan Clough, *The Budapest Convention on Cybercrime: Is Harmonisation Achievable in a Digital World?*, MONASH U. (July 30, 2013), http://www.aic.gov.au/media_library/conferences/2013-isoc/presentations/clough.pdf.

[3] *See* Council of Europe (COE), CONVENTION ON CYBERCRIME, (Nov. 23, 2001), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (last visited Oct. 25, 2016).

[4] Brian Harley, *A Global Convention on Cybercrime?*, COLUM. SCI & TECH. L. REV. (Mar. 23, 2010), http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.

[5] Colin Lecher, *US Reaches Economic Cybersecurity Agreement with China*, THE VERGE (Sept. 25, 2015), http://www.theverge.com/2015/9/25/9399187/obama-china-cyber-security-agreement.

[6] Danielle Correa, *China and the UK Sign Cyber-Security Agreement*, SC MAG., (Oct. 22, 2015), http://www.scmagazineuk.com/china-and-the-uk-sign-cyber-security-agreement/article/448578/.

[7] Kevin Sawyer, *Germany and China Reach Agreement to End Commercial Cyberwar*, NAT'L MONITOR (Oct. 29, 2015), http://natmonitor.com/2015/10/29/germany-and-china-reach-agreement-to-end-commercial-cyberwar/.

[8] Lee Munson, *Russia and China Sign Cyber Security Pact, Vow Not to Hack Each Other*, NAKED SECURITY (May 11, 2015), https://nakedsecurity.sophos.com/2015/05/11/russia-and-china-sign-cyber-security-pact-vow-not-to-hack-each-other/.

the one between the United States and China, can actually be enforced and thus will achieve their stated goals. Moreover, the agreements leave out other vital organizations such as civil society organizations, critical infrastructure, and the government, military, intelligence, and law enforcement organizations of the respective countries.[9]

Finally, attempts have been made to include 'Internet-based surveillance systems' in the Wassenaar Arrangement, a multilateral agreement on export controls for conventional arms and dual-use goods and technologies. The proposals to extend the Wassenaar Arrangement have been criticized on the basis that, in the long run, it would undermine cyber-security by criminalizing the very security research activities that result in the identification and correction of vulnerabilities in software and hardware.

2. *Diffusion of Power.*

One of the megatrends identified by the National Intelligence Council in its report, *Global Trends 2030: Alternative Worlds*, is the increasing diffusion of power globally.[10] In this increasingly multipolar world, power shifts to networks and coalitions made up of non-state actors such as private enterprises and individual threat actors such as hackers. Ironically, this diffusion and dispersion of power is partly driven by vast improvements in communication technologies. These conditions make it difficult to implement and enforce international agreements even when there is general consensus and agreement on a specific cyber security policy at the international level.

"Who do I call if I want to call Europe", is a quote commonly misattributed to Henry Kissinger in reference to the difficulty in international relations and negotiations when dealing

[9] Richard Bejtlich, *To hack, or not to hack?*, BROOKINGS (Sept. 28, 2015), https://www.brookings.edu/blog/up-front/2015/09/28/to-hack-or-not-to-hack/.

[10] *See Generally Global Trends 2030: Alternative Worlds*, NAT'L INTELLIGENCE COUNS. (Dec. 2012), https://www.dni.gov/index.php/about/organization/global-trends-2030.

with a dispersed entity that has no single representative. The quote nicely encapsulates the current problem facing cyber security policy at an international level between nation states: there is simply no one body or entity to call or to convene major stakeholders to address cyber security threats or challenges.

The international diplomatic system has trouble integrating the views of entities outside of the Westphalian system of nation states. The Internet is a decentralized network of networks that involves privately owned entities in almost all countries. In this aspect, the Internet's greatest strength inherently incorporates its greatest weakness; designed to survive a nuclear conflict, redundancy is baked into its very structure but at the expense of the ability for central administration. As with the nation state system itself, there is no central controlling actor or actors capable of forcing compliance on all participants. International negotiations require the participation of these private entities, yet the international system is not built to incorporate such actors, and so remains unable to include them in ways essential to the success of any treaty in this domain. And yet without the inclusion of such groups and individuals, any international agreement is doomed to failure from the outset.

In fact, this diffusion of nation state power is compounded by the very 'empowerment of the individual' that the Internet itself facilitates. This term refers to the way that digital technologies invert traditional power dynamics. Now individuals, with very few resources, are able to influence the actions and behavior of governmental or multinational organizations many times their own size. Suicide bombers provide a dramatic example of this phenomenon. The influence of individual non-state actors is particularly relevant in cyber security. Many of the threat actors in this field are organized criminal outfits, in many cases backed explicitly or tolerated by the state in which they reside. Widespread availability and adoption of commercially available information communication technologies grants individuals capabilities to access and amplify information previously only available to nation states. And destructive effects are not limited only to organized groups, but can reside within the reach of individual hackers themselves as well.

Effectively controlling such a system through a slow moving and rigid set of decision-making rules, procedures and processes, such as those that characterize the international system, is an immensely difficult task. Even were binding agreements to be reached, actual implementation of these agreements presents a whole new set of difficulties. And enforcement proves harder still, especially in the fast-moving technological landscape. These is a deep and persistent, perhaps unfathomable breach, between the speed of government and bureaucratic action, and that of technological innovation. In such a contest, technology is bound to circumvent particular restrictions long before those constraints can be implemented. And this is likely to be true for the foreseeable future.

B. National

In organizations there are at least four reasons why planners tend to fail when attempting to address complex problems.[11] First, people tend to oversimplify the process of problem solving to save time and energy.[12] Second, people are overconfident in their own abilities, and thus try to repeat past successes.[13] Third, people have trouble quickly absorbing and retaining the large amounts of information necessary to understand dynamic, ever-changing processes.[14] Finally, people tend to focus on immediately pressing problems at the expense of considering longer term or more distant challenges or the unintended consequences and problems that solutions can create.[15]

These four characteristics of poor decision-making help us understand why the current approach to cyber security policy making at a national and organizational level is failing.

[11] *See* DIETRICH DÖRNER, THE LOGIC OF FAILURE: RECOGNIZING AND AVOIDING ERROR IN COMPLEX SITUATIONS (Basic Books 1989).

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

1. *No National Strategy.*

In the United States, there is no national strategy and no long-term strategy for cyber security policy. This creates a vacuum of responsibility and an absence of direction and constraint which leads to contradictory policy. This inevitably generates the emergence of turf wars over the rapidly expanding Federal funds available for programs nominally meant for 'cyber' purposes, but often directed toward other only tangentially related interventions by agencies which seek to co-opt these funds for other purposes.

This is not a new problem, nor one restricted solely to the domain of 'cyber' for that matter. In 2013, the Government Accountability Office released a report entitled, '*National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*'.[16] Specific problems identified with the cyber security policy approach include: few milestones or performance measures in government strategy documents; the assignment of high-level roles and responsibilities but important operational details being left unclear; and wide variance across cyber security strategy documents in terms of priorities and structure, how they link to or supersede other documents, and how they fit into an overarching national cyber security strategy.[17] Little has changed to improve these deficits in the intervening years.

The Department of Defense's Cyber Strategy, perhaps the longest standing national strategy document, provides a set of strategic goals but lacks fine-grained, operational details that are publicly available.[18] The Comprehensive National Cybersecurity Initiative was released in 2013 and came with 12 initiatives but did not come with an operational plan on how these initiatives should be

[16] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-187, CYBERSECURITY: NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED (2013).

[17] *Id.*

[18] *The DOD Cyber Strategy*, THE DEP'T OF DEFENSE (Apr. 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

implemented and operationalized.[19] The Cybersecurity National Action Plan came with a set of actions, like setting up a Commission on Enhancing National Cybersecurity, and creating a Federal Chief Information Security Officer position, and allocated $19 billion in funds across a plethora of activities, but did not include tangible outcomes and metrics for determining cost effectiveness or 'success'. This is a combination tailor-made for inciting misuse of government funds.

The responsibilities for portions of cyber security policy are spread out across dozens of Federal agencies, the Department of Defense and intelligence community, regulators and other ancillary bodies (like Information Sharing and Analysis Centers, or ISACs). This dispersed responsibility, coupled with no overarching strategy, creates situations where agencies pursue cyber security policy goals that match their organization's interests but, in many cases, contradict the cyber security concerns of other organizations, sectors, and people, or produce unnecessary, wasteful, or even deleterious redundancies, often even without awareness of such duplication. Lack of fully transparent communication between these divisions within the government serves to further complicate problems associated with disaggregated policy planning and implementation.

A recent example is the push by FBI Director Comey for laws that would mandate backdoors to be placed in encryption standards. Were this policy to be successfully implemented, it would have the effect of weakening overall cyber security (including the cyber security of other government agencies), not to mention the ability of foreign actors to access sensitive American materials.

Another example is the National Security Agency, which has a dual mission that in practice is contradictory. The Signals Intelligence mission requires that the agency acquire the communications of foreign governments (espionage). The second mission of the NSA, the Information Assurance mission, tasks the agency with safeguarding the information of government agencies,

[19] *The Comprehensive National Cybersecurity Initiative*, EXECUTIVE OFF. OF THE PRESIDENT OF THE U.S., https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited Sept. 25, 2016).

corporations and individuals in the U.S. The approach is summarized as 'keep our information safe, get theirs.'

The Signals Intelligence mission requires that key information technology infrastructure, hardware and software, be weakened and exploited. These technologies, in many cases are the same ones used by government agencies, corporations and individuals in the United States itself. The weakening of these technologies puts these entities in the U.S. at risk (the revelation in 2016 of back-doored Juniper routers, which are used by many U.S. Federal government departments, is a case in point). Add to this the fact that US Cyber Command, which is the military's designated organization for safeguarding its networks and information, is led by the same person that leads the NSA, and we have a muddled set of responsibilities with little coordination.

C. Organizational

1. *Lack of Evidence Base.*

Evidence-based policy making is an approach where policy decisions are based on the collection and interpretation of objective evidence relating to the policy issue at hand and the performance of the policy option implemented. Its intellectual roots lie in evidence-based medicine, where randomized controlled trials are used to assess the policies or treatments that contribute most toward the resolution of a particular condition or ailment. This etiology embodies an important corrective; fixing one problem in the human body often causes another because systems are enmeshed in ways that are not always obvious, clear or systematic. Similarly, in a network design like the Internet, focusing on simple, easy-to-measure outcomes can quickly become a version of the drunkard's search. Just as lowering cholesterol does little to change overall risk of coronary artery disease, although the ability to do so with statins makes billions for Big Pharma every year, reducing the number of hacks may not necessarily mean the overall system is safer. After all, body counts in Vietnam did little to provide an accurate indicator of how well the United States was doing in that war. Effective decision-making in complex environments requires knowledge about the structure of a system and the outcomes of the decisions made in relation to the goals that are being pursued.[20] Without this knowledge, an organization may implement interventions that ultimately exacerbate the very problems that it seeks to mitigate.

In cyber security policy, there is a dearth of reliable, verifiable data on the financial scale of the losses, the sources of threats and risks, and the potential positive and negative impacts of policy decisions. While figures on the number of cyber incidents are released annually by the Computer Emergency Response Team (US-CERT), such figures are methodologically questionable – for instance - much of the increasing incidence figures could be chalked up to better detection methods and companies have incentives to hide serious breaches - and thus give very little in the way of policy-relevant guidance.

Where there are metrics available, there is no guarantee that they will be actionable, relevant or useful. For instance, since 2003 the Department of Homeland Security has been operating an intrusion detection system, formerly called the National Cybersecurity Protection System, now called the EINSTEIN program.[21][22] After over a decade of operation, and $6 billion in investment, "none [of the metrics developed by DHS] provide insight into the value derived from the functions of the system."[23] An estimated $19 billion was allocated to cyber security measures in the 2017 White House budget proposal, representing a 35% increase

[20] *See* DÖRNER, *supra* note 11.

[21] It is of great concern therefore that the Cybersecurity National Action Plan calls for the Department of Homeland Security to enhance Federal cybersecurity, "by expanding the EINSTEIN and Continuous Diagnostics and Mitigation programs".

[22] Aliya Sternstein, *US Homeland Security's $6B Firewall Has More Than a Few Frightening Blind Spots*, DEFENSE ONE (Jan. 29 2016), http://www.defenseone.com/technology/2016/01/us-homeland-securitys-6b-firewall-has-more-few-frightening-blind-spots/125528/.

[23] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-294, INFORMATION SECURITY: NHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM (2016).

over the previous year.[24] However, it was not clear where all these funds were going because there was no definition for what actually constitutes a 'cyber security program'.[25] Even data on research and development (R&D) spending on cyber security, the release of which is required by law, have only been made available as recently as 2013.[26]

The lack of reliable evidence is due to a number of reasons. There are strong incentives for corporations and government agencies not to disclose whether an information security failure has occurred, facilitated in part by patchy data breach notification laws, which are set at a state level in the United States, and differ substantially in their requirements. Companies may not want competitors to know their weaknesses, and corporations as well as the government may not want the public to lose faith that their personal financial, medical, or social information is safe when they interact with them. This of course assumes that the company is aware of a failure in information security having even taken place, which is far from guaranteed.

Where there are data and studies available, the most commonly cited data sources are compiled by security or antivirus vendors, who have business incentives to magnify the problem, or are in studies undertaken by academic institutions or think tanks and sponsored by corporations that operate in the field. These studies make unrealistic assumptions about the behavioral responses of companies, and do not take into account the unobserved differences among companies in the datasets. They assume that all companies react in the same way to information security incidents regardless of industry, size (whether by headcount or annual revenues), business model or current revenues, costs or profitability. In reality, the losses

[24] *The President's Budget for Fiscal Year 2017*, THE WHITE HOUSE: OFF. OF MGMT. AND BUDGET, https://www.whitehouse.gov/omb/budget (last visited Sept. 26, 2016).

[25] *Middle Class Economics: Cybersecurity*, THE WHITE HOUSE: THE PRESIDENT'S BUDGET, FISCAL YEAR 2016 (Aug. 7, 2015), https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity-updated.pdf.

[26] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

that a company might face from a security breach are influenced by the individual company's fragility, which in turn is a function of a number of firm-level characteristics including customer loyalty, profit margins or debt. For a hypothetical example, if a company with low profit margins, low customer loyalty and high debt is subject to a costly data breach, and that information becomes public, the periodic drop in revenues and curtailed access to short-term debt might render the company insolvent. This would not be the case for a company with high margins, high customer loyalty and low debt. Yet many studies treat all companies as if they were identical when predicting or forecasting potential impacts of a breach.

Selection bias is also endemic. The only companies that appear in malware or data breach incident datasets are those that: a) detected the incident; b) subsequently reported the incident; and c) were able to accurately quantify the impact of the incident. Of the entire universe of companies, only a fraction of a fraction is likely to be included in this analysis. Simple methodological problems like ensuring a representative sample are endemic in commonly used, self-reported surveys. The total losses across countries are often based on extrapolations for entire populations; multiplying the average loss per company by the total companies in the country or economy may not provide the most accurate estimate of actual breaches or losses.[27]

This lack of evidence means that cyber security policy makers cannot determine where the true problems lies and where policy interventions might have the greatest benefit given their costs, nor can they track the subsequent outcomes of the policy interventions that they make. This failure then compounds over years as successful policy interventions aren't identifiable and failed policy interventions are allowed to persist in spite of their failure.

With no basis on which to evaluate the need for and effectiveness of cyber security policy, there is a risk that the system becomes nothing more than a 'self-licking ice cream cone': A self-

[27] Dinei Florencio & Cormac Herley, *Sex, Lies and Cyber-crime Surveys* (Microsoft Research, Working Paper), *available at* https://www.microsoft.com/en-us/research/wp-content/uploads/2011/06/SexLiesandCybercrimeSurveys.pdf.

perpetuating process that is meant to address a problem but instead contributes to the very problem that it is ostensibly designed to solve.

2. *Chronic Lack of Technical Knowledge.*

The chronic lack of technical knowledge and talent within the organizations with responsibility for cyber security policy severely hampers these organizations' ability to effectively develop and implement policies. This technical knowledge gap can be attributed to there being no standard way in which to classify or keep track of cyber security related roles, and to the inability of Federal agencies to retain and develop what technical talent they are able to hire.

Again, this problem is not new. In 2011, the Government Accountability Office released a report titled '*Cybersecurity Human Capital: Initiatives need Better Planning and Coordination*', flagging that, "eight agencies with the biggest IT [information technology] budgets have trouble handling their cybersecurity workforces and determining their composition and responsibilities."[28] It remains a persistent problem. In a 2013 report, the GAO wrote that, "only 2 of 8 agencies it reviewed developed cyber workforce plans and only 3 of the 8 agencies had a department-wide training program for their cybersecurity workforce."[29] The Department of Defense was the only agency to report their shortage to the GAO in 2011 (as they were the only ones who had a methodology in place).

This has not stopped government agencies from announcing large hiring targets, complete with large budgets, to hire cyber security personnel. The Department of Defense announced that it would have 6,000 'cyber-warriors' by 2016 but there is little indication of where these people would come from (much less what a 'cyber-

[28] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-8, CYBERSECURITY HUMAN CAPITAL: INITIATIVES NEED BETTER PLANNING AND COORDINATION (2011).

[29] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

warrior' does). The Office of Personnel Management was also competing to hire 1,000 cyber security personnel in this market.[30]

The Department of Homeland Security is the private sector's liaison on cyber security matters – it also advises other agencies on the issue. The GAO identified 1,361 cyber security personnel at DHS in their 2013 study. One official is quoted as saying, "the National Cyber Security Division has had trouble finding personnel for certain specialized areas, such as watch officers".[31] This division has a central role in operating important interventions such as the EINSTEIN system, developing the National Cyber Incident Response Plan, and operating the National Cybersecurity Center.

The lack of any data to measure the problem or outcomes of policies to address the problem makes achieving strategic goals, like Initiative #8 of the *Comprehensive National Cybersecurity Initiative*, which calls to, "develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees," even more challenging.

Another underlying reason for the chronic lack of technically skilled people in government is that government can rarely compete with the private sector in the IT arena in terms of salary, stock options, prestige and other remunerations. Few career public servants have an advanced understanding of technical issues in the area of cyber security, and even fewer private sector IT professionals have any understanding of, much less interest in, the processes underlying the formulation of government policy. At a cultural or ideological level, many of those who work in or are a part of the tech industry either in Silicon Valley or more generally have a Libertarian or Randian bent. They are broadly skeptical of and distrust government,[32] exacerbating the conflict between government and industry in the surveillance versus privacy debate around cyber security goals. Even if the government could compete head-to-head

[30] GOVERNMENT PUBLISHING OFF., https://www.gpo.gov/fdsys/pkg/FR-2015-11-10/html/2015-28566.htm (last visited Sept. 26, 2016).

[31] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 16.

[32] A compact summary of this set of values can be found in Richard Barbrook and Andy Cameron's 1995 essay 'The Californian Ideology'.

in pay, it would still have to overcome the ideological forces that dissuade Silicon Valley from collaborating openly with government.

The security and screening requirements for many positions related to cyber security in the Federal government have created obstacles to hiring talent as well. One example is Ashkan Soltani, who was in line to work with the White House's Office of Science and Technology Policy after a stint as the Federal Trade Commission's Chief Technologist, but whose security clearance application was rejected possibly due to past affiliation with Edward Snowden.[33] In another example from 2014, the Director of the Federal Bureau of Investigation stated that the agency was considering relaxing its policy, which prohibited hiring anyone who had used cannabis in the past three years, because it was so difficult to find candidates for cyber security roles who would pass the policy's requirements.[34]

Simultaneously, private entities with the skill base to address some of these challenges technologically have no ostensible reason to include policy experts on their design teams. Government does not mandate or regulate such participants, and there is little or no support or infrastructure in most technology companies for their contribution. On the other side of the equation, it is hard enough for the government agencies to find people to manage and secure their internal information technology networks, let alone find those with the technical knowledge and skills coupled with an understanding of public policy formulation and implementation. Both sides are thus confronted with enormous challenges to achieving mutual understanding and translation of basic needs and goals.

Finally, government organizations typically set their cyber security policy internally as a list of compliance-based check boxes that the system administrators are expected to rigidly follow. These

[33] Danny Yadron, *White House denies clearance to tech researcher with links to Snowden*, THE GUARDIAN (Jan. 29, 2016), https://www.theguardian.com/technology/2016/jan/29/white-house-tech-researcher-denied-security-clearance-edward-snowden-nsa.

[34] Leo Kelion, *FBI 'could hire hackers on cannabis' to fight cybercrime*, BBC NEWS (May 22, 2014), http://www.bbc.com/news/technology-27499595.

check box lists are developed from the perspective of the defender, not the adversary, so they are typically circumvented by highly resourced and sentient adversaries. Their 'one size fits all' approach emphasizes attaining compliance over actually directing resources towards areas where dynamic risks are greatest for the organization in question.

The management of government agencies also does not permit the system administrators who manage their IT networks the autonomy necessary to take a proactive approach to system security. These rigid policies are the equivalent of handcuffing the security guard at the front of the building and then telling him/her to keep the place safe from thieves. A long-term effect is that, rather than empowering the system administrators to proactively address cyber security concerns, this approach drives out the most talented technical employees, thereby compounding the already acute skills shortage in Federal agencies.

D. Individual

1. *Heuristics and Biases.*

Clearly many challenges confront our ability to formulate effective cyber-security policy. Not least among these are systematic and predictable barriers which exist in the minds of individual decision makers and other stake-holders. A few of these merit some comment, specifically roadblocks related to loss aversion and the difficulties of making decisions under conditions of uncertainty. These proclivities can induce a kind of paralysis because people find themselves averse not only to change, but especially to risks and threats that incorporate some element of uncertainty.

Loss aversion constitutes a well-known phenomenon first experimentally documented in the work of Daniel Kahneman and Amos Tversky.[35] This work elegantly demonstrated human hedonic

[35] *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis Of Decision Under Risk*, 47 ECONOMETRICA: J. OF THE ECONOMETRIC SOC'Y 263, 261-

asymmetry. In short, people are more averse to loss than they are attracted to an equal gain. So, for example, it hurts more to lose $10 than it makes most people happy to win $10. In fact, people need to be offered about $25 on average to make them indifferent between a bet which can lead to a loss of $10. In other words, most people need two and a half times more potential benefit in order to take the risk of a potential loss. This phenomenon in and of itself can, of course, lead to a particular kind of paralysis since it embodies an inherent status quo bias. People will of course seek out uncomplicated gains, but if a path also poses a risk, people will, on average, show a relatively high degree of loss aversion.

There is, however, one important consistent exception, as described in Prospect Theory.[36] When people are operating in a so-called domain of losses, when things are bad and look to be getting worse, people become much more prone to taking risks, including quite dramatic ones, in order to recoup previous losses, and return to the former status quo position.

There are a couple of important caveats in this work. Most relevant, people will show the opposite tendency, meaning risk aversion in the domain of losses, when probabilities are low. This explains, for example, the almost universal acceptance of insurance whereby people pay a sure cost to avoid the very small probability of a larger loss. But note there that these assessments of likelihood typically result from subjective assessments and not necessarily objective probability, meaning that people can often misjudge how likely a given event may be. This would certainly be especially likely in a domain such as cyber-security where the base rate of risk is largely unknown as we noted above. While it makes sense that any given company or entity may want to keep successful attacks secret, this lack of transparency makes it much more difficult for the overall community to accurately assess the objective threat and share important information on successful defensive strategies. This secrecy works to the attackers' advantage. Greater dissemination of accurate information about kinds and types of attack, even within

91 (1979); *see also* Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341, 341-50 (1984).

[36] *Id.*

closed networks, might allow for the development of more effective counter-strategies, or even more effective insurance policies to amortize risk across the broader system, even if such allocation were restricted to specific sectors or industries.

In policy terms, this translates into some potentially destructive consequences. In short, people are more likely to take risks that could make things worse precisely when they are already in bad circumstances. This can easily snowball to make things a lot worse very quickly. These are the times when caution might be most warranted, but is also less likely, particularly in an environment permeated by a sense of crisis, time pressure or high stakes. Thus, policy makers may prove loath to develop policies to implement if disaster strikes when things are going well, for fear of offending potential allies and donors, because of distraction from more pressing problems at any given moment, or due to general status quo malaise. However, once a crisis hits, pressure mounts, and that sense of threat and risk is precisely what throws decision makers into a domain of loss where the potential for optimal decision making is restricted, and in the absence of well-developed and rehearsed standard operating procedures, catastrophic losses become much more likely to occur simply as a result of momentum. Under such conditions of attack, risk acceptance dominates, especially because the crisis itself shifts leaders' perceptions regarding the probability of subsequent attack.

This entire process may characterize decision-making in any number of domains but becomes exacerbated by the uncertainty that typically permeates cyber-attacks in particular. Decision making under uncertainty often proves difficult. In general, such decisions, particularly when time is of the essence, are dominated by a series of so-called judgmental heuristics[37] which provide useful rules of thumb for filling in the blanks when objective probabilities remain unknown. Their exact operation remains outside the purview of this discussion and can be found elsewhere.[38] For our purposes, suffice it to say that

[37] Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCI. 1124, 1124-31 (1974).

[38] *See* ROSE MCDERMOTT, RISK TAKING IN INTERNATIONAL POLITICS: PROSPECT THEORY IN AMERICAN FOREIGN POLICY (University of Michigan Press, 1998) (discussing an application to political science).

uncertainty, like risk, can systematically restrict optimal decision making by encouraging individual leaders to revert to established psychological strategies and procedures in decision making that may not be well suited for the given problems or challenges they confront. Recall that such biases evolved precisely because in most circumstances they offer fast and easy and largely accurate responses to the world; in other words, they developed precisely because, on average, they allow largely accurate estimates in the absence of objective information at the lowest cognitive cost. However, it is precisely in novel or unusual circumstances, such as those often posed by cyber-security challenges, where we might expect the systematic operation of such biases to induce predictable biases leading to sub-optimal results.

However, this need not necessarily be the case. Sometimes, embracing the wisdom of uncertainty can precipitate unexpected creativity in decision-making. Admittedly, this is most likely when the decision-making milieu is not riven by time pressures, which is why systematic planning prior to crisis becomes essential to avoid the more negative consequences of psychological bias in decision making. Conversely, when planning can take place at a time of relative security, the acceptance of uncertainty can help generate unexpected solutions and opportunities because individuals come to see that the standard operating procedures do not properly address new challenges which exist in domains divergent from those areas which the original procedures were designed to address. For example, standard operating procedures designed to respond to a military assault on a physical location will not offer much guidance when the attack occurs in virtual space, however real the financial, logistical or operational consequences of cyber breaches. Therefore, it is precisely the inherent uncertainty of the new environment that offers the possibility for new and creative responses, but these are only likely to emerge under conditions of calm, not under circumstances defined by threat and the risk, where loss aversion will dominate, and risky choices become more likely.

Thus, it becomes easy to see how the same pattern of unproductive and unresponsive decision-making recurs. When the problem is not salient, it is easier not to do anything, but under conditions of threat, risky choices predominate, which may not necessarily help future outcomes. As Einstein said, the definition of insanity is doing the same thing over and over and expecting a different result. However, if we change the approach, and embrace the creative possibilities present under conditions of uncertainty in times of calm, it may then become possible to harness human psychological tendencies in our own favor to develop more creative solutions to novel problems.

III. SECTION 3

A. Developing Governance Models that Manage to Diffuse Power and Non-State Actors

The international system has to adapt to a world that is vastly different from that which it was built to manage. Effective cyber security policy development and implementation at an international level will require bringing nation states together with private companies, the technical community, non-governmental organizations, and individual hackers. Faced with diffused power across many linked entities, decision-making structures and processes themselves have to be more adaptable, flexible, bottom-up, and resilient. As with many contemporary global challenges, there is a need for governance mechanisms unlike those that were used to govern the more kinetic international challenges, which dominated international relations prior-to and during the 20th century.

A number of international organizations are attempting to take responsibility for various aspects of cyber security policy at the international level. For example, in 2014, the United Nation's International Telecommunications Union (ITU) called for, "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies."39 The

[39] International Telecommunications Union [ITU] (2014), Resolution 140 rev Busan 2014: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies,

ITU membership brings together governments and the private sector (including Sector Members, Associates and Academia) to forge agreements on radio communications standards and increasing development through greater access to information and communication technologies (ICTs).

The problem for organizations such as the United Nations and other international fora is that they either do not or can only partially include the diverse state and non-state stakeholders that comprise the cyber security field. In addition, their typical programs of work have timelines that span many years. In the time it takes to complete one cycle, a field like cyber security usually moved on to new and more pressing issues.

One model worth examining more closely is the Internet Engineering Task Force (IETF), which has done a good job over the past two decades providing a forum in which technical experts and organizations can come together to make decisions relating to the technical architecture on which the Internet operates. This process has been effective because of its open format – anyone can join the meetings – its rough consensus system for reaching agreement, and the Request for Proposal system, which ensures that all participants have an opportunity to make proposals and then debate these proposals. These characteristics have resulted in technically robust and agreed upon technical standards and outcomes for the Internet.

B. National – A National Cyber Security Plan

Following Dörner's original findings, addressing complex problems requires the establishment of an overall plan with clear goals, a 'systems level' understanding of the environment in which the plan will be executed, and iterative revision of the plan in response to information updates on the state of play. Components of a coherent plan to guide cyber security policy at a national level include a long-term strategy with clear goals, milestones, performance targets, resources, and responsibilities.

https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res. 130.pdf (last visited March 7, 2016).

For the first time, as a follow-up to the 30-day 'cyber sprint',[40] an operational plan was released on October 30, 2015 to upgrade Federal cyber security in the United States. The White House *Cybersecurity Strategy and Implementation Plan (CSIP)* was intended, "to identify and address critical cyber security gaps and emerging priorities, and make specific recommendations to address those gaps and priorities."[41] It had 5 overarching objectives:

- Prioritized identification and protection of high value information and assets;
- Timely detection of and rapid response to cyber incidents;
- Rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Sprint assessment;
- Recruitment and retention of the most highly-qualified cyber security workforce talent the Federal Government can bring to bear; and
- Efficient and effective acquisition and deployment of existing and emerging technology.

[40] After realizing that over 14 million personnel records had been stolen from the U.S. government Office of Personnel Management, a 30 day 'cybersecurity sprint' was announced. The goal was to take, "number of steps to further protect Federal information and assets and improve the resilience of Federal networks". In tangible terms, some steps included the patching of critical vulnerabilities, acceleration of the implementation of multi-factor authentication, and tightening of policies and practices for privileged users. Progress reports were required after 30 days (The White House, 2015c). What's extraordinary is that, after tens of billions of dollars in prior investment, these basic steps had not yet been implemented.

[41] Memorandum from The Executive Office of the President to Heads of Executive Departments and Agencies (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

Each of these 5 objectives was given a set of concrete goals linked to the achievement of the objectives. Its timeline clearly laid out the steps that had to be taken, and allocated responsibility to the respective organizations in order to achieve the stated objectives before September 2016.

This plan was a major first step in a very narrow part of the U.S. Federal Government's efforts to implement basic cyber-security measures among selected Federal departments. This approach should be replicated to cover cyber-security policy nationally for the public and private sectors.

As a part of the development of this plan, a clearer and less contradictory allocation of authority and responsibilities for key portions of cyber security policy is required. The announcement of a Chief Information Security Officer, who focuses on coordinating cyber security across federal agencies, and is housed within the Office of Management and Budget at the White House, is a promising first step in this direction.[42]

However, the announcement of the possibility that the Signals Intelligence and Information Assurance responsibilities within NSA may be merged, two functions that are in practice contradictory, was a possible step in the wrong direction.[43] A far better alternative would have been to allocate the Signals Intelligence mission to the NSA, the government and military Information Assurance mission to US Cyber Command (which would have to be led by a different person than the head of the NSA), and the private sector Information Assurance mission allocated to where it resides at present with the Department of Homeland Security (with the Chief Information Security Officer potentially playing an oversight or coordination role). Such an arrangement would have avoided the

[42] Danny Yadron, *White House seeks its first ever chief information officer*, THE GUARDIAN (Feb. 9, 2016), https://www.theguardian.com/technology/2016/feb/09/white-house-seeks-first-chief-information-security-officer-hackers-cybersecurity-hacking.

[43] Danny Yadron, *NSA merging anti-hacker team that fixes security holes with one that uses them*, THE GUARDIAN (Feb. 3, 2016), https://www.theguardian.com/technology/2016/feb/03/nsa-hacker-cybersecurity-intelligence.

prior conflict of interest by separating the offensive capabilities, by housing them in the Department of Defense, from the defensive capabilities, by housing them in the Department of Homeland Security.

C. Organizational

1. *Improving the Evidence Base.*

More robust evidence would contribute greatly to better cyber security policy and filling the chronic lack of technical knowledge that has emerged in Federal agencies. Creating a mechanism where private companies are required to report breaches while ensuring the secrecy of such information might go far toward creating a more comprehensive data base, while assuring such firms that their leaks would not risk unnecessary public distrust or the exposure of proprietary code or information.

There needs to be standard definitions for what cyber security budget spending actually constitutes and agreed measures for the results or outcomes of these budget items. This is necessary so that money nominally allocated to 'cyber security' is not used for other purposes merely because its meaning can be easily morphed; the result of a policy produced through such aggregation would be haphazard at best, lacking integration and overall strategy. This is akin to asking for the input and output measures for cyber security policies. With these measures in hand, the outcomes of cyber security policy interventions can be evaluated.

Of all fields, development economics might have tools for potential use in testing cyber security policy interventions. For instance, the logical framework approach (log-frames) has been used for decades to design interventions in many complex fields (e.g. agriculture, education, health) by identifying goals, tying actions to those goals, and then evaluating the intervention according to pre-established metrics.[44]

Borrowing from the medical field, development economics and development aid organizations have some well-developed tools and principles for the monitoring and evaluation of interventions in complex systems.[45] Participants are randomly allocated to one of two groups, only one of these groups is given the intervention, and then the differences between the groups post-intervention are measured so as to determine its effectiveness or efficiency. However, as with the human body, the Internet is a large network, meaning that changes in one place may affect other parts of the system in unintended or unanticipated ways, and attention to such feedback loops remains an important part of not making things worse by providing a series of bandages that do nothing to stop the bleeding (or to prevent later problems such as infections).

Lessons from this field could be drawn and deployed to give cyber security policy makers a toolkit with which to classify their budget items in a consistent way (the inputs). This then allows measures of the effects of these policies across metrics like the number of breaches per year, or the proportion of designated high-value information that is encrypted, or any measure that is deemed appropriate (the outputs) to be developed, and used to adjust, eliminate or add various program elements to improve performance.

2. *Specialized Track for Technical Talent.*

To improve the level of technical talent in cyber security roles within government agencies, a specialized track for this talent –

[44] *See* D. McLean, *The Logical Framework In Research Planning And Evaluation* 1-11 (ISNAR, Working Paper No. 12, 1988); *see also Guidance on using the revised Logical Framework*, DEPARTMENT FOR INT'L DEV. (Jan. 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253889/using-revised-logical-framework-external.pdf.

[45] *See* Esther Duflo & Michael Kremer, *Use of Randomization in the Evaluation of Development Effectiveness*, http://economics.mit.edu/files/2785 (last visited Sept. 27, 2016); *see also* Abhijit V. Banerjee & Esther Duflo, *The Experimental Approach to Development Economics*, 1 ANN. REV. ECON. 151, 151-78 (2009).

subject to different working conditions and hiring requirements than typical positions – is one avenue worth exploring. Indeed, as part of the Cybersecurity National Action Plan (CNAP), a $62 million educational fund was created, "for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal government."[46] This was an extension of the already-established National Science Foundation's and Department of Homeland Security's CyberCorps Scholarship for Service program and a sort of Reserve Officer Training Corps program for new cyber security talent.[47] Such a program provides long term benefits to recipients as well as government agencies as a larger pool of experts is recruited and cultivated.

Other existing initiatives might provide lessons for this or other special training initiatives. One might be the US Digital Services (USDS), which was originally modeled on the United Kingdom's Government Digital Service. The USDS is housed within The White House Office of Management and Budget that brings technical, policy and legal professionals and places them in Federal agencies where technical talent is lacking. They take a human centered design approach to the use of technology to make government departments more responsive and accessible to people. They have projects running in areas that have been deemed priorities by the Obama administration including Veteran's Affairs, Department of Homeland Security (linked to immigration, not cyber security), Social Security and the IRS. Their annual budget is partially covered by Congress and partly comes from the partner agencies where their members work.

Another model that might be worth emulating is the Jefferson Science Fellowship Program. This program has existed since 2003 and allows tenured, or similarly ranked, academic scientists, engineers and physicians from U.S. institutions of higher learning to spend one year in Washington D.C. at the U.S.

[46] *The President's Budget for Fiscal Year 2017*, *supra* note 24.

[47] *See* Sean Gallagher, *Obama wants you to join CyberCorps Reserve to help feds get their act together*, ARS TECHNICA (Feb. 9, 2016), http://arstechnica.com/tech-policy/2016/02/obama-wants-you-join-the-cybercorps-reserve-to-help-feds-get-their-act-together/.

Department of State or the U.S. Agency for International Development (USAID). A similar program might be developed for cyber security talent, in U.S. higher education establishments or even private sector companies (given that some of the best talent resides in the financial sector), to do a yearlong service in government agencies where their technical talent or specialized knowledge could be used to improve the organization's cyber security or strategy in this area. Such a program might also potentiate important and on-going social networks between government and technical experts, and allow each to achieve a greater understanding of the other's needs, incentives, goals and constraints.

Each of these programs may not be able to compete financially with the private section, but by harnessing existing talent, supporting emerging talent, and trying to attach service and prestige to government work, such strategies can help to improve the current reservoir of skill within existing agencies.

D. Individual

Of course, the structural incentives identified can be shifted through organizational changes to induce greater compliance and attention to issues surrounding cyber security, including enhanced transparency and improved integration and communication across agencies tasked with different but overlapping goals. But ultimately the causal agents within any organization are individuals who remain subject to the inherent psychological biases we discussed above.

1. *Transparently Structured Choices and Consequences*.

It is not easy, but there are some standard ways to reduce individual's susceptibility to such biases.[48] First among these is simply to make people aware of the unconscious biases that may affect their judgment and decision-making. The simplest way to do this is not through complicated, time-consuming, expensive training programs during which people zone out. Rather, the idea is to make sure that

[48] *See supra* note 35, at *Id.*

choices are structured in a transparent way so that such biases become evident. For example, in the classic experiment where people had to make real life choices between radiation and surgery for cancer, options were presented with "mortality" and "survival" statistics side by side. When this is done, the equivalency of the options becomes immediately evident, but the psychological pull across framing also remains obvious. In a similar manner, choices between options in response to a particular threat should present both the costs and benefits of options side by side, not only for the relevant choices, as is often typically done, but also relative to the status quo (i.e. doing nothing) option so that costs and consequences of inaction become as immediately salient as those associated with any given course of action.

Because people are preternaturally preoccupied with loss, it is important to find ways to convey not only probabilities, but also help people to better understand how to psychologically calibrate the meaning of abstract probabilities. The human mind does not do well with very large numbers; we are all aware of the phenomenon of "crisis fatigue" whereby one dead boy on a beach is a tragedy but hundreds of thousands of refugees pouring into Europe from Syria is an immigration challenge that provokes border controls and political hostility.

These numeracy challenges can play out in myriad ways. One of the best ways to help decision makers contemplate very large data breaches is to encourage strategies or procedures for transforming such issues into very direct and small scale terms. Human psychology is much better suited for solving smaller scale problems; it is much easier for people to get a handle on and contemplate how to respond in a constructive way to challenges that are framed in local terms. So, for example, we can worry about threats to the electrical grid but the initial policy problem that needs to be solved and addressed might be better facilitated if it was framed in terms of how to get electricity back up in Washington, D.C. without cyber capacity, and then scale up from these more local decisions to national policy plans.

2. *Training through Gaming and other Table-Top Simulations for Emotion Regulation.*

Importantly, as much as the Western canon has taught professionals to privilege rationality over emotion, rationality as posited by economists in particular is little more than an intellectual construct completely devoid of psychological reality. Psychological rationality is deeply emotional by design; the human mind privileges emotional information since that is what has been key to survival in the face of myriad threats over millennial time. This means that people are exquisitely sensitive to emotional inputs, perhaps overly so in modern contexts, but as with loss aversion, we are more attentive to negative emotions such as fear and anger than more positive ones such as hope and joy.

Negative emotions, while important and useful for helping us to properly allocate energy and attention, and also to consolidate memory, can nonetheless encourage over-reactions to threats and attacks, especially uncertain ones that pose an ambiguous or uncertain risk. Encouraging training for emotion regulation would be time and money well spent to reduce the risk of over-reaction to uncertain or threatening stimuli. Enormous amounts of evidence now exist documenting the benefits of mindfulness based stress reduction strategies in achieving such goals.[49]

Moreover, this is a domain in which gaming and other table-top simulations positing different kinds of threats and crises could prove helpful in giving people an engaging, even fun, way to gain practice, experience and knowledge about potential response options to any given scenario. Such strategies also work to build a sense of community and camaraderie among those who would have to work together in a real crisis. In this way, issues of dominance, specialization of labor and other issues which can interfere with effective, time-sensitive responses, can be negotiated prior to the actual crisis, so that when real challenges emerge, team coordination and cooperation can be as smooth as might reasonably be expected.

[49] *See* P.R. Goldin & J.J. Gross, *Effects of mindfulness-based stress reduction (MBSR) on emotion regulation in social anxiety disorder*, 10 EMOTION 83, 83-91 (2010).

IV. SECTION 4

Research will be required to translate many of the proposals made in the section above into the cyber security policy field. This section outlines a research agenda that is intended to provide some guidance on the kinds of research questions that might profitably be pursued and the research methods that might help yield useful answers.

A. Developing Governance Models that Manage to Diffuse Power and Non-State Actors

An examination of governance models that have either been designed to coordinate diffuse entities, or that have proven to be successful in coordinating diffuse entities, would be a useful step forward in determining a global governance model for cyber security policy. This paper has already mentioned the IETF as a model that has proven successful in the past for managing technical matters related to the Internet globally.

Perhaps there are lessons to be drawn from global governance models in other areas of public health policy, such as the World Health Organization and the Centers for Disease Control, or in conflict mitigation and resource sharing, such as the Arctic Council, or in the establishment of international law, such as the United Nations Conventions on the Law of the Sea?

A comparative examination of these varied arrangements would look at the types of parties involved, the mechanisms by which decisions are made and consensus is achieved, the cost of setting up and maintaining the mechanism (and by whom this cost is borne), the success of the mechanism in achieving its stated objectives, and the reasons for failure should failure be experienced.

One of the challenges with devising a new set of governance strategies with the flexibility and adaptivity that would allow both state and non-state actors, including businesses, to engage is that the Internet itself, as a network of networks, and the World Wide Web, run contrary to most established forms of government structure, which are hierarchical in nature. While originally hailed as a mechanism to survive and enhance resilience in the case of nuclear war, and later as a means by to encourage and facilitate greater democratic involvement, the Internet also provides a platform where individuals with very few resources can exert almost unprecedented damage and destruction. This structure challenges those who wish to provide an interface between hierarchical and horizontal governance structures to offer a different kind of structure.

One kind of structure that might potentially be considered involves the notion of panarchy as developed by Buzz Holling and colleagues[50] in their work on environmental sustainability. This work developed out of examining how systems in nature achieve balance across large systems over time. In this concept, three factors of capacity, connectedness and resilience emerge most prominent.

The Internet itself offers almost limitless potential for connectedness and great potential for resilience, but this framework raises stark concern about the relative capacity of predator and prey. However, this is where another biological model might prove useful and instructive. Well-established equations such as the Lotka-Volterra[51] which characterizes the predator-prey dynamic would allow similar mathematical modeling of the dynamic interaction between hackers, governments and the businesses who try to survive and thrive in cyber space. Although originally developed in a biological context to represent the impact of disease and competition among animals as a function of numbers, time and rates of interaction to measure prospects for survival or extinction, it has long been used in

[50] C.S. Holling, *Understanding the complexity of economic, ecological, and social systems*, 4 Ecosystems 390, 390-405 (2001); Brian Walker et al., *Resilience, adaptability and transformability in social-ecological systems*, 9 Ecology and Soc'y (2004).

[51] A.J. Lotka, *Contribution to the Theory of Periodic Reaction*, 14 J. OF PHYSICAL CHEMISTRY 271, 271-74 (1910); A.J. Lotka, *Analytical Note on Certain Rhythmic Relations in Organic Systems*, 6 PROCEEDINGS OF THE NAT'L ACAD. OF SCI. OF THE U.S. 410, 410-15 (1920); A.J. LOTKA, ELEMENTS OF PHYSICAL BIOLOGY, 71-274 (Williams and Wilkins, 1925); VITO VOLTERRA, VARIATIONS AND FLUCTUATIONS OF THE NUMBER OF INDIVIDUALS IN ANIMAL SPECIES LIVING TOGETHER (R.N. Chapman ed., 1931).

economics to model interaction of sectors in industries as well,[52] and could readily be adapted for use in the context of cyber competition. It has more recently been used successfully to characterize the maintenance of cultures of honor in environments with aggressive actors and weak institutions, a condition not unlike the current state of Internet governance.

This model offers important insight because although it makes a number of important simplifying assumptions, it also highlights how the evolution of predator and prey influence each other. In an evolutionary context, predators select for characteristics that will enhance their ability to find and capture prey, just as prey select for traits that increase their ability to hide, escape or otherwise evade predation. These selection features influence the oscillation dynamics of each side in the equation, precipitating cycles of dominance, but because the goals of predator and prey are antagonistic, the selection of mutually antipathetic characteristics profoundly affects the dynamics of their interaction as well as prospects for survival. These biological models, which exist in well-developed differential equations, and have already been used to positive effect in economics, offer concrete ways to examine the interaction between hackers and defenders, regardless of which sides governments or businesses may be on.

B. A National Cyber Security Plan

The first step in developing a national cyber security plan requires examining what has been done in other countries in the past, as well as seeking to develop innovative solutions for our own particular needs and goals. To date, there is limited comparative literature on the national cyber security plans deployed in countries such as Singapore's 5 year National Cyber Security Masterplan, the United Kingdom's National Cyber Security Strategy, and Canada's Cyber Security Strategy, among many others.

[52] R.M. Goodwin, *A Growth Cycle*, *in* SOCIALISM, CAPITALISM AND ECONOMIC GROWTH (C.H. Feinstein ed., 1967).

Comparing the success of other country's plans - which have clear goals, action plans, metrics for success, timelines and responsible agencies - would allow for a comprehensive plan to be written in the United States that learns from the successes and failures of others (rather than repeating any recognized mistakes).

C. Specialized Track for Technical Talent

The first step in considering new policy proposals should be a pre-feasibility study based on cost-benefit analysis. A cost-benefit analysis would look at the financial cost, both to the host organization that would pay for the awardee's stipend, and to the organization from which the awardee is seconded. It then becomes possible to compare this dollar amount to the benefits that would accrue to the host organization and to the alternative policy option of training or hiring talent from scratch. If the costs outweigh the benefits by a certain ratio, then this policy option may not be worth pursuing.

The point of comparing this specialized track to training or hiring from scratch is important. The major strength of creating a specialized track for bringing technical talent into government for the short-term, vis-à-vis the current approach, which is epitomized by proposals to hire 6,000 'cyber warriors' into DoD or 1,000 new personnel into OPM, is that it is will not run into the practical resource constraints that are going to face these other proposals (namely: that there simply aren't enough qualified people in work force to hire at this level for the medium-term). Indeed, a cost-benefit analysis will likely find that the cost effectiveness of a specialized track is many times less than the alternative, which would have the added benefit of freeing up funds to be used for other initiatives with the goal of bolstering cyber security.

D. Improving the Evidence Base

Compiling transparent, reliable, and statistically rigorous cyber security statistics would contribute to better decisions in cyber security policy. The problem to date has been that this responsibility has been taken on either by organizations with a stake in stoking greater fears about cyber security (e.g. anti-virus companies and private security vendors) or with organizations that lack the requisite statistical capacity to provide reliable data (e.g. the FBI's Internet Crime Complaint Center).

This is typical practice in the U.S., where statistics are compiled by organizations responsible for the regulation of the sector or administration of the sector (e.g. the Federal Aviation Authority compiles aviation data, similarly the National Center for Health Statistics operates under the Centers for Disease Control). Assigning a disinterested party with sufficient statistical capacity and credibility to provide an independent assessment of the scale of the problem could prove very helpful for beginning to design programs to help address these issues. Could the National Institute for Standards and Technology play a role, either as a convener or as an authority to grant some authority to cyber security data?

When randomized control trials were applied from medicine to the development economics field in the late 1990s, there was a need to develop a specialized methodology to respond to the unique logistical and ethical issues that arise in international development work. Adjustments to randomized control trial methodologies will likewise have to be made to adapt them to the unique characteristics of cyber security.

For instance, it isn't clear how comparable control and treatment groups might be identified or separated when so many network elements differ across organizations (indeed, even within organization the elements are likely to differ). The rate at which the technology changes and software is patched might also make it difficult to keep the two groups separate and, within the groups, maintain consistency across subjects (then again, many organizations run on legacy systems that are 10 years old, so this might not be such a great obstacle depending on the organization). This might imply that the studies might only be able to be conducted at the organization-level, though we simply don't know yet.

An assessment of the costs of running an experiment would be useful. The costs of randomized control trials in cyber security may not be cost-effective. The up-front costs to actually run the experiments may not be overwhelming, especially considering the multi-billion dollar budgets being allocated at a national level, but the cost associated with the losses to the control group may accrue over time and offset the potential gains from the experiment (then again, given that attackers only need to infiltrate one out of potentially thousands of users to compromise a system, perhaps the risk levels remain the same whether undertaking an experiment or not, although the cost may not).

A taxonomy of cyber security 'inputs' and 'outputs' would also have to be developed in order to undertake an experiment. Accurate measures for the effects of treatment would also need to be developed and established. The goal would be to determine which metrics exist and can be reliably measured, or which ones might have to be created, in order to measure effectively the various policy interventions that could be made to reduce certain cyber security risks.

E. Developing Gaming and Other Table-Top Simulations

There is a long and established body of work on gaming and table-top simulations for crisis situations, even in cyber security. Indeed, a recommendation during a panel on mitigating cyber security threats at a recent conference at Columbia University was that, "simulations, war/business games, and table-top exercises can provide additional venues for information sharing and help build trust between participants, which can be helpful in crisis situations."[53]

Indeed, this is where using the intrinsic strengths of the industry itself may be able to potentiate innovative methods for training and testing; the use of simulations can prove enormously helpful by providing a way to control for many elements while

[53] *Proceedings of the Conference on Internet Governance and Cyber Security*, COLUMBIA SCH. OF INT'L AND PUB. AFF. (May 14, 2015), https://sipa.columbia.edu/system/files/Proceedings_ColumbiaSIPA_InternetGoverance_Cybersecurity_Conference2015.pdf.

varying one, and being able to do so across many diverse elements quickly, either simultaneously or sequentially. Once problematic areas are identified using this strategy, more elaborate real time experiments can be conducted manipulating potentially problematic aspects. Any such simulations could be easily conducted using existing Internet based platforms which allow for multi-user simultaneous interaction.

Where new research might be especially useful is in the development of methods that combine psychological training and emotion regulation training with simulations. The idea would be to run through the several stages that comprise risk-based approaches to cyber security, such as the NIST Risk Management Framework, so as to identify where the failure to successfully implement the framework occurs due to panic or individual biases and heuristics, and then address these sources of failure.

V. CONCLUSION

We have described the factors that we believe influence decision making in the area of cyber security across four main levels of analysis: international; national; organizational; and individual. Each poses unique challenges to the development of a coherent and consistent policy of cyber security.

After describing what has been done to enhance cyber security at each level, and noting the challenges that remain, we have suggested some important ways in which policy and research might advance policy in more productive ways. These include: establishing a coherent national plan with clear and coherent benchmarks and policies and plans for implementation and accountability; the conscious development of different governance structures for regulating the Internet internationally; creating a national service action plan for recruiting and circulating cyber talent in and out of government; providing a more accurate evidence base of past experience to improve future response; and establishing regular games and simulations to train people in how to respond to differing potential threats.

Enhancing cyber security is a critically important project. It also appears an overwhelming one on which we have made less progress than those who seek to exploit the systems in question. In developing systems designed more for overall resiliency than security, the architects of the Internet never imagined the widespread use it would achieve. However, this resilience has also resulted in vulnerabilities that now need to be addressed. It will require a great deal of coordinated action on the part of many individuals, users, industry and government actors to improve cyber security without compromising privacy unduly. Working diligently and creatively to achieve such a goal will help make everyone safer and more productive.