DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD

TASK FORCE ON CYBER DETERRENCE

February, 2017

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense (DoD). The DSB Study on Cyber Deterrence completed its information-gathering in December 2016. The report was cleared for open publication by the DoD Office of Security Review on February 23, 2017. This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE UNDERSECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

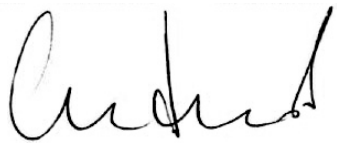
SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence

I am pleased to forward the final report of the Defense Science Board Task Force on Cyber Deterrence, co-chaired by Dr. James N. Miller and Mr. James R. Gosler.

This body of work represents a two-year study effort by its accomplished members who have sought to identify the requirements for effectively deterring both costly cyber intrusions and the full range of cyber attacks. If implemented, the recommendations in this report – some reinforcing ongoing DoD efforts and many others proposing new activity – will bolster U.S. cyber deterrence and strengthen U.S. national security.

The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed.

I fully endorse all of the Task Force's recommendations contained in this report, and urge their careful consideration and soonest adoption.



Craig Fields
Chairman, Defense Science Board

Attachment:
As stated

THIS PAGE LEFT INTENTIONALLY BLANK

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence

The final report of the DSB Task Force on Cyber Deterrence is attached.

The Cyber Deterrence Task Force was asked to consider the requirements for deterrence of the full range of potential cyber attacks against the United States and U.S. allies/partners, and to identify critical capabilities (cyber and non-cyber) needed to support deterrence, warfighting, and escalation control against a highly cyber-capable adversary.

Public interest in cyber deterrence has grown over the past several years as the United States has experienced a number of cyber attacks and costly cyber intrusions. However, it is essential to understand that cyber attacks on the United States to date do not represent the "high end" threats that could be conducted by U.S. adversaries today – let alone the much more daunting threats of cyber attacks and costly cyber intrusions that the Nation will face in coming years as adversary capabilities continue to grow rapidly.

The Task Force determined the United States faces three distinct sets of cyber deterrence challenges.

First, major powers (e.g., Russia and China) have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks. This emerging situation threatens to place the United States in an untenable strategic position. Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. The U.S. military itself has a deep and extensive dependence on information technology as well, creating a massive attack surface.

Second, regional powers (e.g., Iran and North Korea) have a growing potential to use indigenous or purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure. The U.S. Government must work with the private sector to intensify efforts to defend and boost the cyber resilience of U.S. critical infrastructure in order to avoid allowing extensive vulnerability to these nations. It is no more palatable to allow the United States to be held hostage to catastrophic attack via cyber weapons by such actors than via nuclear weapons.

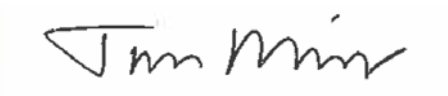
Third, a range of state and non-state actors have the capacity for persistent cyber attacks and costly cyber intrusions against the United States, which individually may be

inconsequential (or be only one element of a broader campaign) but which cumulatively subject the Nation to a "death by 1,000 hacks."

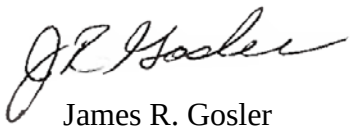
To address these challenges, bolstering the U.S. cyber deterrence posture must be an urgent priority. The DoD and the Nation should pursue three broad sets of initiatives to bolster deterrence of the most important cyber threats and related challenges to the United States.

1. **Plan and Conduct Tailored Deterrence Campaigns**: The U.S. cyber deterrence posture must be "tailored" to cope with the range of potential attacks that could be conducted by each potential adversary. And it must do so in contexts ranging from peacetime to "gray zone" conflicts to crisis to war. Clearly, for U.S. cyber deterrence (as with deterrence more broadly), one size will not fit all.
2. **Create a Cyber-Resilient "Thin Line" of Key U.S. Strike Systems**: The DoD must devote urgent and sustained attention to boosting the cyber resilience of select U.S. strike systems (cyber, nuclear, non-nuclear) and supporting critical infrastructure in order to ensure that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks. In effect, DoD must create a second-strike cyber resilient "Thin Line" element of U.S. military forces to underwrite deterrence of major attacks by major powers.
3. **Enhance Foundational Capabilities**: In addition to the measures outlined above, the Department of Defense and the broader U.S. Government must pursue several different types of capabilities, such as enhancing cyber attribution, the broad cyber resilience of the joint force, and innovative technologies that can enhance the cyber security of the most vital U.S. critical infrastructure.

If implemented and sustained over time, this report's recommendations – some reinforcing ongoing DoD efforts and many others proposing new activity – will substantially bolster the U.S. cyber deterrence posture, thereby reducing risks to the Nation.



James N. Miller
Co-Chair



James R. Gosler
Co-Chair

Attachment:
As stated

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

Introduction

The United States gains tremendous economic, social, and military advantages from cyberspace. However, our pursuit of these advantages has created extensive dependencies on highly vulnerable information technologies and industrial control systems. As a result, U.S. national security is at unacceptable and growing risk.

Over the past several years, the United States has been subjected to cyber attacks and costly cyber intrusions by various actors, including the four most cyber-capable adversary states identified by the Director of National Intelligence (DNI) in 2016.[1] For example:

- During 2012–2013, Iran conducted distributed denial of services attacks on Wall Street firms, disrupting operations and imposing tens of millions of dollars in remediation and cyber hardening costs.[2]
- In 2014, North Korea hacked Sony Pictures in an effort to suppress the release of a movie depicting a plot to assassinate North Korean leader Kim Jong Un, causing direct and indirect financial damage in the process.[3]
- For at least 10 years,[4] China conducted a massive cyber theft of U.S. firms' intellectual property (IP); since President Xi Jingping committed in September 2015 that China would not undertake such theft; reportedly Chinese cyber IP theft has reduced but not stopped.
- In 2016, Russia hacked into several U.S. institutions and used the resulting stolen information in an attempt to undermine voter confidence and affect the outcome of the U.S. presidential election.[5]
- Non-state actors, though generally less capable than nation-states, also have conducted cyber attacks. A recent example is the October 2016 distributed denial of service attacks on the internet domain name system (DNS) provider Dyn, for which the hacker groups Anonymous and New World Hackers claimed responsibility.[6]

---

[1] Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement; 9 February 2016

[2] Department of Justice press release "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector"; 24 March 2016

[3] "The North Korean Threat: Nuclear, Missiles and Cyber"; 13 January 2015 testimony before the House Foreign Affairs Committee by the Special Representative for North Korea Policy

[4] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07. Additional reports are located at the website of the National Counterintelligence and Security Center

[5] Assessing Russian Activities and Intentions in Recent US Elections; ICA 2017-01D; 6 January 2017

[6] New World Hackers group claims responsibility for internet disruption; CBS News; 22 October 2016

Each of the above examples stands out from the constant barrage of cyber intrusions that occur in the United States and globally on a daily basis, including those conducted by nations as part of their cyber espionage programs. Such actions qualify as cyber "attacks" (Iran's Distributed Denial-of-Service Attack (DDoS) and North Korea's Sony hack) or costly cyber intrusions (China's intellectual property (IP) theft and Russia's hack of political parties to facilitate information operations) because their impact goes beyond data collection, to impose some form of harm on the United States.

Of critical importance, known cyber attacks on the United States to date do not represent the "high-end" threats that could be conducted by U.S. adversaries today – let alone the much more daunting threats of cyber attack the Nation will face in coming years as adversary capabilities continue to grow rapidly. A large-scale cyber attack on civilian critical infrastructure could cause chaos by disrupting the flow of electricity, money, communications, fuel, and water. Thus far, we have only seen the virtual tip of the cyber attack iceberg.

Report Terminology

To discuss the concept of cyber deterrence, it is important to establish some common terminology.

Cyber. Cyber elements include all digital automation, including those used by the Department of Defense (DoD) and its industrial base. This includes information technology (IT) embedded in weapons systems and their platforms; command, control, and communications (C3) systems; intelligence, surveillance, and reconnaissance (ISR) systems; logistics and human resource systems; and mobile as well as fixed-infrastructure systems. "Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident on or operating within any DoD system environment, which are commonly collectively referred to as information and telecommunication technology (ICT).[7]

Cyber Attack. For the purposes of this report, a cyber attack is any deliberate action that affects the desired availability and/or integrity of data or information systems integral to operational outcomes of a given organization. Not all cyber intrusions constitute attacks; indeed the vast majority do not. Cyber attacks may have temporary or permanent effects; they may be destructive of equipment or only disruptive of services; and they may be conducted remotely or by close access (including by insiders). In addition, while there is considerable attention given to cyber attacks focused on data and software-in-operation, supply chain vulnerabilities are of growing concern in a world where critical infrastructure is

[7] DSB Task Force on "Resilient Military Systems and the Advanced Cyber Threat;" January 2013"

built and sustained through a global supply chain subject to malicious alteration across various phases of system life cycles.[8]

Costly Cyber Intrusions. Under our definitions, China's massive cyber theft of U.S. intellectual property and Russia's hack of U.S. political parties to facilitate information operations undermining confidence in U.S. elections represent costly cyber intrusions. The cyber intrusions in these cases did not affect the availability and/or integrity of U.S. data or information systems, and so do not constitute cyber attacks, but these intrusions did facilitate unacceptable actions by China and Russia that imposed respectively economic and political costs on the United States.

Deterrence. Deterrence operates by affecting the calculations of an adversary, specifically by convincing the adversary that the expected costs of a potential act (a type of attack or costly cyber intrusion) outweigh the expected benefits. *Deterrence by denial* operates by reducing the expected benefits of attack, while *deterrence by cost imposition* operates by increasing the expected costs. The two types of deterrence, by denial and by cost imposition, are not alternatives to each other; both are important to an effective deterrence posture. On one hand, steps to promote deterrence by denial – for example by improving cyber defenses and increasing resilience of key systems to attack – can apply to multiple adversaries and do not depend on high-confidence attribution. Deterrence by cost imposition, on the other hand, requires the ability to attribute with high confidence, the perpetrator(s) of an attack in order to credibly threaten assets (i.e., things they hold dear) to a degree that is sufficiently consequential to individuals associated with the attack; and to communicate in advance both the will and capability to impose such costs in response to the attack(s) or exploitation(s) one wants to deter.

Cyber Deterrence. Quite simply, for the purpose of the Task Force, cyber deterrence is the use of both deterrence by denial and deterrence by cost imposition to convince adversaries not to conduct cyber attacks or costly cyber intrusions against the United States, and in at least some instances, to extend this deterrence to protect allies and partners.

Just as cyber is a relatively new domain, cyber deterrence is a relatively new endeavor. For the most part, to date the United States has been establishing its cyber deterrence posture step-by-step, in response to attacks. Although the United States responded with diplomatic moves and economic sanctions to North Korea's Sony hack, China's IP theft, and Russia's meddling in U.S. elections, it is far from clear that such responses have established effective deterrence of future cyber attacks and costly cyber intrusions.

[8] Defense Science Board Task Force on Cyber Supply Chain; November 2016

Indeed, it is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed.

At the same time, it is important to understand that not all cyber attacks or costly intrusions will be deterrable. As one important example, even the certain promise of severe punishment may not deter terrorist groups bent on wreaking havoc on the United States and our allies. As a second and quite different example, if the United States were in a major war with another nation, we should not expect to be able to deter even debilitating cyber attacks on U.S. military capabilities that produced little or no collateral damage to civilian society; as discussed in detail below this reality suggests the central importance of ensuring key military strike capabilities are cyber second-strike resilient to even an all-out cyber attack by an advanced adversary.

Key Cyber Deterrence Challenges

What is cumulatively taking shape are three critical cyber deterrence challenges:

- Major powers' (e.g., Russia and China) significant and increasing ability to hold U.S. critical infrastructure at risk or otherwise use the information domain to harm vital U.S. interests, and their more limited but growing capability to thwart our military response through cyber attack;
- Lesser powers' (e.g., Iran and North Korea) and potentially non-state actors' possible ability, through increasingly available cyber tools—indigenous, purchased, or transferred—to conduct catastrophic attacks on U.S. critical infrastructure; and
- A range of state and non-state actors' growing capacity for persistent cyber attacks and costly cyber intrusions against the United States, which individually may be inconsequential (or be only one element of a broader campaign) but which cumulatively subject the Nation to a "death by 1,000 hacks."

The United States must strengthen its cyber deterrence posture against these three critical challenges – and do so by focusing on the specific actors who pose these challenges. While progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, improvements are not on a pace to reduce risks to acceptable levels within the next decade. The introduction of massive numbers of digital sensors (the so-called Internet of Things), processors, and autonomous devices to today's internet will only exacerbate an already tenuous posture and make defense even more challenging in the coming years. The unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures.

Over the past several years, the U.S. Government, and particularly the DoD, has taken a range of valuable steps to bolster the U.S. cyber deterrence posture. However, it will take many more years of effort, consistent senior-leader attention, and a sufficient budget for ongoing and planned steps to come to fruition. Moreover, additional steps are urgently needed.

If implemented, the recommendations in this report – some reinforcing ongoing DoD efforts and many others proposing new activity – will help accelerate the strengthening of U.S. cyber deterrence.

Guiding Principles

In working to bolster the U.S. cyber deterrence posture, the DoD and broader U.S. Government should take account of a number of guiding principles:

- **The U.S. cyber deterrence posture must include both deterrence by denial and deterrence by cost imposition, with a different balance depending on the perpetrator and the severity of the attack to be deterred.** Deterrence by denial operates through a combination of defenses and resilience to attack, so the adversary understands they will not succeed in the aims of its contemplated cyber attack. Deterrence by cost imposition operates when the adversary believes the United States has both the credible will and capability to respond to a cyber attack with a response (military and/or non-military) such that the expected costs to the adversary exceed the expected benefits of an attack; both are essential.

- **Deterrence by cost imposition requires understanding what key adversary decision makers value, holding that which they value at risk, and communicating (explicitly and/or implicitly by precedential action) the credible will and capability to respond.** A decision to conduct – or not conduct – a cyber attack on the United States will not be taken by a country; rather, it will be taken by a leader or small leadership group, and this leader or group must be the focus of U.S. deterrence planning.

- **Deterrence by cost imposition requires credible response options at varying levels of conflict.** Because "massive retaliation" to limited cyber attacks by nuclear-capable adversaries such as Russia and China is not credible, the United States must develop cyber and non-cyber proportional (although not necessarily symmetrical) response capabilities to attacks, ranging from low-level disruption to catastrophic destruction and loss of life. While offensive cyber responses are an essential part of the toolkit, the full range of military responses (symmetric or asymmetric) – as well as diplomatic, law enforcement, and economic responses – must also be considered.

- **In the event of a cyber attack on the United States (i.e., a failure of cyber deterrence), the question should not be whether to impose costs in response, but how and when to do so against the attacker, and how to connect the response to the attack.** Following this guiding principle reinforces the need for high confidence attribution capabilities, as well as an extensive array of resilient military and non-military response options. This guiding principle does not apply to cyber espionage, which may or may not provoke a response beyond defensive measures. (The United States views cyber espionage as a legitimate activity, and undertakes it extensively; yet, just as with espionage conducted by human spies, there should be both limits and consequences to being caught.)

- **The United States must clarify, first internally and then to potential adversaries, that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions**. Theft of IP and hacking in support of undermining U.S. political institutions are now clearly on the list; there are numerous other contenders. One example is egregious behavior in conducting cyber espionage: just as there are sanctions for crossing unwritten rules of traditional espionage, so there may be in the cyber domain. Some would view the 2015 cyber heist from the Office of Personnel Management of some 18 million records containing personal information as so egregious as to warrant a strong U.S. response. A second example is the pre-positioning of malicious software in critical systems, for example the HAVEX[9] and BlackEnergy[10] malware discovered in the U.S. electrical grid. In the view of this Task Force, although egregious cyber espionage and the insertion of malware in critical systems of the U.S. electrical grid may not constitute cyber attacks, the United States must consider how such malign acts might be deterred.

- **Responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation (and quite possibly intelligence loss), but not responding carries near-certainty of suffering otherwise deterrable attacks in the future.** Responding to a cyber attack requires balancing between taking action that is so weak that it invites further attacks, and action so strong that it causes unneeded escalation and a loss of support domestically and among U.S. allies and partners. However, for two key reasons, U.S. leaders must not be paralyzed into inaction by fear of escalation. First, the risk of escalation applies to the adversary as well as to the United States; it is part of what makes deterrent threats more potent. Second, a failure to respond to cyber attacks is an invitation to follow-on cyber attacks of (at least) a similar nature and scope, which may be even more escalatory over the long term than responding in a compelling manner.

- **Reducing the vulnerability of U.S. critical infrastructure is essential not only to deterrence by denial, it also reinforces the credibility of U.S. threats to impose costs on attackers**. It is broadly understood, both among U.S. policymakers and potential adversaries, that due to our extreme dependencies on vulnerable information systems, the United States today lives in a virtual "glass house." Hardening and increasing the resilience of the most vital critical infrastructure systems – including electricity, water, and waste water – is urgently needed to bolster deterrence by denial and by cost imposition.

[9] Havex Trojan: ICS-ALERT-14-176-02A
[10] BlackEnergy: ICS-ALERT-14-281-01E

- **Although it may appear desirable in theory to find effective arms control approaches to stabilize the cyber balance between major powers – U.S.-Russia and U.S.-China – in practice cyber arms control is not viable, though norms and rules of the road may be both viable and highly valuable.** Due to the nature of cyber systems and attack tools, the verification of cyber arms control limitations would not be feasible. However, if the United States can clearly define norms and rules of the road by which it is willing to abide in crisis and conflict (progress has already been made on establishing international cyber norms in peacetime), then we can and should build such rules into our cyber deterrence posture including declaratory policy. Such steps, while difficult, may be the best alternative to an unabated cyber arms race.

Bolstering the U.S. cyber deterrence posture must be an urgent priority. The DoD and the Nation should pursue three broad sets of initiatives, as outlined in the following sections, to bolster deterrence of the most important cyber threats and related challenges to the United States.

1. Plan and Conduct Tailored Deterrence Campaigns

The United States faces significant cyber threats from a number of potential adversaries, most notably from Russia, China, Iran, North Korea, and terrorist groups including the Islamic State of Iraq and Syria (ISIS). These actors have the potential to undertake a wide variety of cyber attacks, ranging from theft of IP, to distributed denial of service attacks, hacks of private sector companies or public institutions, disruption of U.S. military operations, and catastrophic attack on critical civilian infrastructure.

The U.S. cyber deterrence posture must be "tailored" to cope with the range of potential attacks that could be conducted by each potential adversary. And it must do so in contexts ranging from peacetime to "gray zone" conflicts to crisis to war. Clearly, for U.S. cyber deterrence (as with deterrence more broadly), one size will not fit all.

Conducting detailed advance planning for responses to every plausible cyber attack, with every potential adversary in every conceivable scenario, is neither possible nor necessary. Nor is it feasible to have in hand the "optimal" response to each hypothetical attack scenario. However, it is both possible and essential to conduct systematic planning and wargaming, to establish clear employment and declaratory policies, and to establish priorities for the development of a range of potential cyber and non-cyber (and military and non-military) responses to cyber attacks.

Campaign planning for cyber deterrence should consider the "most likely" types of attacks. Today, a wide range of actors may undertake cyber attacks which individually are only slightly disruptive or destructive, but which over time can subject the United States to "death by a 1,000 hacks" and impose cumulatively high costs while undermining our credibility of response to more impactful individual attacks. Russia and China have both been part of the problem to date, and could take this threat to the next level by using cyber in sustained campaigns to undermine U.S. economic growth, financial services and systems, political institutions (e.g., elections[11]), and social cohesion. While U.S. "whole-of-government" response options have been used (e.g., diplomatic expulsions, criminal prosecutions, economic sanctions), a wider range of military cyber options, and a clear policy and legal framework for their employment, is needed to add essential rungs to the U.S. escalation ladder. Finally, while tailored campaigns will necessarily define some unique components for the given adversary, every campaign derives significant benefit from the common foundation(s) of resilience and deterrence by denial recommended in this report.

[11] Russia's Influence Campaign Targeting the 2016 US Presidential Election; ICA 2017-01D; 6 January 2017

Campaign planning for cyber deterrence must also consider the "most dangerous" types of attacks by our potential adversaries; for example, widespread sustained destructive attacks against U.S. critical infrastructure. Such attacks would clearly constitute an act of aggression and likely an act of war. An adversary would almost certainly be aware of this reality, and so likely seek to degrade not only U.S. offensive cyber capabilities, but to the extent it was able to, delay, degrade, and where possible, deny U.S. military capabilities. This set of challenges is addressed in detail in Section 2 of this report.

The Strategic Context for Crisis and Conflict in the Emerging Cyber Era

The United States and Russia, and the United States and China, share extremely strong stakes in avoiding major war, including through misperception and inadvertent escalation. The dynamics of cyber offensive weapons will increase challenges to crisis stability, as each side is likely to perceive significant advantages and relatively low risks (no direct casualties, no visible damage) to going first with offensive cyber against the other side's military. At the same time, one side's assessment of imminent/underway offensive cyber attacks against its offensive cyber capabilities or military more broadly could be viewed as a compelling indicator of imminent conflict – and create real fears of "use or lose." Thus, as offensive cyber capabilities continue to grow, and are likely to outpace cyber defense and resilience, there are likely to be growing risks of misperception that could lead to rapid cyber escalation – and the potential for rapid escalation to armed conflict. Because benefits of offensive cyber are large and growing, arms control verification is impossible, and attribution is challenging, this issue is not going away. However, conducting detailed planning and wargaming can help identify ways to reduce such risks, for example by defining key military systems for protection, establishing norms or "rules of the road," and continuing and expanding bilateral discussions of the future of strategic stability.

1.1 Pursue Adversary-Specific Campaign Planning and Wargaming

Findings:

Because deterrence operates by affecting the calculations of specific decision-making individuals in another nation or group – the goal being to convince these decision makers that the expected costs of an attack outweigh its expected benefits – deterrence planning must focus on what key leaders on the other side value, and on how they are likely to make decisions. Some adversary leaders may place highest value on the security and economic well-being of their people; in other cases they may place significant value on their own financial well-being or status.

DoD's priority focus for cyber deterrence should be on key leadership individuals (including those who influence them) in the top four cyber threat nation-states: Russia, China, Iran, and North Korea. ISIS and other terrorist groups are pursuing more advanced cyber capabilities;

however deterrence of cyber (or other) attacks by such groups may not be possible in many scenarios, so that prevention/preemption and defense should be the principal U.S. approach.

A campaign perspective is needed in order to better deter future attacks, to avoid under-reacting or over-reacting to specific incidents, and to drive the prioritization of both defensive and offensive capabilities. It is essential that cyber deterrence planning not focus only on one-off events (such as a large-scale attack on civilian critical infrastructure), but be formulated as a campaign that is continuous. In one sense, the United States has a campaign underway today to deter cyber attacks – but to date, that campaign has been largely reactive and not effective.

A critical element in strengthening the U.S. cyber deterrence posture is the clarification of norms regarding the implantation and employment of offensive cyber weapons. Many if not most cyber exploits – whether intended to facilitate the collection of intelligence or to facilitate a later attack – require clandestine intrusion well in advance of any action in order to achieve an objective or effect. However, the subject of such exploits may not be able to discern whether the intent is "legitimate" espionage/collection activities or pre-positioning of disruptive or destructive tools.

As a key example, is it acceptable or unacceptable for nations to pre-position malicious software in each other's electrical grids, as appears to have occurred to the United States with "HAVEX" and "BlackEnergy" malware? If it is acceptable, then the United States may wish to take such actions – if for no other reason than to deter an adversary from "pulling the trigger" on similar implants it may have placed in U.S. systems. If it is unacceptable, then the United States should work to identify and impose costs on any nation that undertakes such an action.

Gaining clarity within the U.S. Government regarding norms concerning the implantation and employment of offensive cyber weapons is essential to appropriate capability development, to forming an effective declaratory policy and engaging allies and adversaries, and to responding in a clear and consistent manner to cyber attacks on the United States. Moreover, of critical importance, norms provide the basis for international legitimacy for imposing sustained costs on violators – critical for sustaining a long-term campaign.

Although each potential adversary actor has different motivations, values, and decision processes, there is an important distinction between Russia and China on the one hand, and Iran and North Korea on the other.

The United States must lean heavily on cost imposition for deterring Russia and China cyber threats. Credible attribution capabilities and highly cyber-resilient military response options are essential enablers. Although accelerating improvements to cyber defenses and resilience

is vital to strengthen the U.S. posture and provide an essential foundation for deterrence by cost imposition, it will not be possible (for the foreseeable future) to deny highly capable actors the ability to conduct catastrophic cyber attacks on the United States. This is primarily because the limited U.S. efforts to defend U.S. information systems to date are unlikely to accelerate (in the near- to mid-term at least) to the point where they can offset the combination of major powers' technical wherewithal, vast supply of resources (including a supporting intelligence apparatus), and the ability to influence supply chains and exploit vulnerabilities at scale.

However, the United States could – and must – aim to deny North Korea and Iran the ability to undertake catastrophic attacks on U.S. critical infrastructure via cyber, just as the United States aims to deny them the ability to attack with nuclear weapons. Indeed, the United States should pursue this objective aggressively. It is unpalatable to leave the United States vulnerable to catastrophic or coercive attack when it is avoidable – and it is avoidable vis-à-vis North Korea and Iran. The U.S. capability to impose costs is essential but (as in deterring nuclear attack) should be additive to denial.

Recommendations:

- **Under Secretary of Defense for Policy (USD(P)), in coordination with the Chairman of the Joint Chiefs of Staff (CJCS)**: Develop for Secretary of Defense, and then Presidential, approval:
  - A policy framework for cyber deterrence including: updated declaratory policy relating to U.S. responses to cyber attack and use of offensive cyber capabilities, guidance for the employment of offensive cyber, a public affairs plan, and an engagement plan for adversaries and allies. Updated declaratory policy should clarify, for example, that the United States will respond to all cyber attacks and to certain specified types of costly cyber intrusions by imposing costs on those responsible that exceed any benefit that the attacker/intruder may have hoped to gain.
  - Proposed norms for the conduct of offensive cyber operations, in crisis and conflict. These norms will provide boundaries for U.S. planning, and also "red lines" for adversary behavior. The United States must determine internally what norms it wishes to promote, and then engage allies and potential adversaries. In addition to supporting effective cyber deterrence, defining appropriate norms will help U.S. policymakers determine how to reduce incentives among major powers for cyber arms racing and to reduce mutual incentives for preemptive cyber actions in crisis.
  - Guidance for the development of cyber deterrence campaign plans focused on the key leadership of Russia, China, Iran, and North Korea. This guidance should include

a timeline for initial plan development, DoD and then interagency review, Presidential approval, and implementation all within six months. The "steady state" aspects of each plan should go immediately into execution. These plans will need to be adapted over time, and a first update should be provided within six months after implementation. The cyber deterrence campaign plans should be linked, and subordinate, to broader policy guidance and campaign planning relating to deterrence and engagement plans for these four countries; this will require an interagency effort and particularly close collaboration among (preferably a small senior-level group from) DoD, the intelligence community, and the State Department.

- Examination through analysis and gaming of escalation dynamics in various scenarios, as well as the spiral escalatory effects of nations developing increasingly potent offensive cyber capabilities, and what steps should be undertaken to bolster stability in cyberspace and more broadly stability between major powers.

- **Commander U.S. European Command, Commander U.S. Pacific Command, and Commander U.S. Central Command, supported by Commander U.S. Cyber Command (USCYBERCOM)**: In response to guidance developed by USD(P) and approved by the Secretary of Defense and President: Within six months, develop two closely related products: 1) cyber deterrence campaign plans focused on the key leadership of Russia, China, Iran, and North Korea, which include a "steady-state" (day-to-day) plan, and crisis/conflict branches; 2) supporting "whole-of-government" adversary-specific "playbooks" of response options to cyber attacks and costly cyber intrusions on the United States or its interests, ranging from low level hacks to major attacks, including cyber and non-cyber military responses, and potential non-military responses. These playbooks are intended to provide flexible response options for the Nation in response to cyber attacks and costly cyber intrusions during peacetime – as well as to support operations in crisis and war. Assess key risks and risk mitigation, including risks of unintended effects, escalatory response(s), compromising a tool or capability, and to other U.S. Government objectives.

1.2 Develop Additional Cyber and Non-Cyber Rungs on the Escalation Ladder

Findings:

While responding to substantial cyber attacks is clearly essential, even limited foreign government cyber attacks or costly cyber intrusions on the United States, if unanswered, undermine U.S. credibility and ally/partner confidence. Therefore it is important to respond appropriately to all attacks in the broader context of their relevance to the strategic

interests of the United States, whether one-off, or in the context of a broader campaign undertaken by one or more adversaries.

The United States must systematically develop a portfolio of both cyber and non-cyber ("whole-of-government" including diplomatic, economic, law enforcement, and military) response options to a wide range of potential cyber attacks and costly cyber intrusions. The objective should not be to develop a "cookbook" with formulaic responses, but a "playbook" that will allow DoD and other departments to ensure that there is real capability behind the U.S. cyber deterrence posture, and to be able to rapidly provide the President with a range of cyber and non-cyber response options in situations where deterrence fails. In order to support timely decision-making, the "plays" in this playbook must be in the context of a clear policy and legal framework for their employment (including policy and legal vetting and evaluation via interagency wargaming and discussion), as discussed in Section 1.1 above.

Recommendations:

- **USD(P) in coordination with CJCS and General Counsel**: Develop for Secretary of Defense approval and high-level interagency consideration guidance for development of a "whole-of-government" playbook for responses to a range of cyber attacks and costly cyber intrusions on the United States. This guidance should be informed by intelligence assessments of what potential adversary leaders value, and be driven substantially by planning conducted by relevant Combatant Commands (CCMDs) (as discussed in the preceding section). Playbook options must be evaluated not only with respect to their expected direct effects, but also regarding potential cascading effects and escalation dynamics.
- **Commander USCYBERCOM**: Develop specific capabilities to support approved "playbook" options, including capabilities that do not require "burning" intelligence accesses (sources and methods) when exercised. Provide for review and approval by Secretary of Defense, through the USD(P).
- **Director of Cost Assessment and Program Evaluation:** Conduct capability assessment as part of annual program review to ensure prioritization of investments to support the development of "playbook" options.

1.3 Develop Scalable Strategic Offensive Cyber Capabilities

Findings:

The United States should continue to reserve the right to respond to cyber attack and costly cyber intrusions with the full range of its national capabilities, including diplomatic censure, law enforcement actions, and economic sanctions in addition to military action.

However, for three key reasons the United States must maintain – and be seen to maintain – an array of scalable offensive cyber capabilities – including high-impact strategic cyber attack options – as an integral part of its cyber deterrence posture. First, it is inherently credible, and explainable to allies and partners, to respond to a cyber attack with a cyber counter attack. Second, cyber attacks – unlike most other responses – may be clandestine or covert, allowing the possibility for quiet punishment known to the adversary leadership that does not "box them in" politically to a follow-on response. Third, it would be irresponsible for DoD to not provide the President with some discrete (i.e., specific and distinct), and if desired discreet (i.e., under the radar), cyber options, in instances when "kinetic" military action may otherwise be contemplated. Cyber offers the potential for subtle and reversible effects when desired, and for more substantial effects when necessary.

Rapidly establishing and sustaining an array of scalable offensive cyber options, including strategic cyber options, will require a different approach to acquisition. Unlike precision-guided munitions, cyber weapons cannot be bought and deployed on a delivery system (or placed in a storage site) with confidence that they will work when needed. A highly talented cadre of cyber warriors must work together closely with intelligence specialists and technologists in a highly classified environment. And because target systems and software can change, sometimes unexpectedly and at a moment chosen by the adversary, a quick reaction capability with flexible acquisition authorities will be essential.

Recommendations:

- **USD(P) in coordination with CJCS and General Counsel**: Develop guidance for Secretary of Defense approval and issuance directing the Commander USCYBERCOM to develop scalable strategic offensive cyber capabilities, in support of a) deterrence of cyber attack against U.S. critical infrastructure; b) broader deterrence of an attack against the United States and our allies or partners; c) deterrence of cyber campaigns or events such as IP theft, and attempts to influence U.S. elections. These strategic offensive cyber capabilities should hold at risk a range of assets that the adversary leadership is assessed to value.

- **Deputy Secretary of Defense and Vice Chairman of Joint Chiefs of Staff**: Establish a small temporary task force (tiger team) to develop options and recommendations for improved and accelerated acquisition of scalable offensive cyber capabilities, including additional authorities to USCYBERCOM, and the establishment of a small elite rapid/special acquisition organization. Require the task force to report its recommendations within 30 days, and after Secretary of Defense approval of recommendations, continue to track implementation milestones and capability development.

1.4 Concluding Comments

The United States, as well as our allies and partners, are at serious and increasing risk of severe cyber attack and increasingly costly cyber intrusions. The requirement for enhanced deterrence is, in our view, not debatable. Nor is the need to accelerate the implementation of deterrence measures.

Campaign planning for cyber deterrence will certainly be challenging for several reasons. First, each potential adversary might conduct any of a broad range of cyber attacks, in widely varying contexts from peace, to "gray zone" conflict, to severe crisis, to conflict. Second, cyber deterrence campaign planning must be part and parcel of a broader political-military campaign relating to each potential adversary leadership team; actions in the cyber domain affect, and are affected by, other diplomatic and military actions. Third, the effects of cyber attacks can be highly uncertain (even after the fact), and attribution may be challenging in some cases.[12] Fourth, planning must engage senior national security leaders, whose time is limited, to make difficult judgments under tremendous uncertainty about a range of issues including adversary leadership views, the risks of escalation in varying contexts, and the specific impacts of both adversary and U.S. cyber actions on the strategic interests of the United States.

However, these challenges do not mean that cyber campaign planning is not possible, or that effective responses are beyond our reach. Rather they mean that such planning should be undertaken aggressively, focused at the outset on the most likely attacks (particularly those somewhat similar to what we have already experienced) and most dangerous risks (those that represent a reasonable worst-case for each adversary). Because it will take some time to do well, it is essential that this planning start in earnest now by making these plans a very high priority.

[12] Director of National Intelligence James Clapper argued in early 2017 that: "We currently cannot put a lot of stock, at least in my mind, in cyber deterrence. Unlike nuclear weapons, cyber capabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence in my view." January 5, 2017 testimony to Senate Armed Services Committee. DNI Clapper's comments reinforce the importance of having credible non-cyber as well as cyber responses to cyber attacks.

2. Create a Second-Strike Cyber Resilient "Thin Line" Element of U.S. Military Forces

Russia and China are increasing their already substantial capabilities to hold U.S. critical infrastructure at risk by cyber targeting of inherently vulnerable ICT and industrial control system (ICS) architectures. In the face of these ongoing efforts, the U.S. Government and the private sector should continue to intensify their efforts to defend and boost the cyber resilience of U.S. critical civilian infrastructure. However, even with sustained improvements, such progress will not be adequate to deny Russia and China the ability to unleash catastrophic cyber attacks on the United States, given their massive resources, and capabilities-at-scale (e.g., intelligence apparatus, ability to influence supply chains, and ability to introduce and sustain vulnerabilities) to dedicate to their objectives.

Barring major unforeseen breakthroughs in the cyber defense of U.S. civilian critical infrastructure, the United States will not be able to prevent large-scale and potentially catastrophic cyber attacks by Russia or China; for the foreseeable future, we will have to rely heavily on deterrence by cost imposition.

In bolstering our cyber deterrence posture relative to major powers, the United States must account for another reality: over the coming years, Russia and China will also be working to increase their ability through cyber attack (and other means) to delay, disorganize, disrupt, and where possible negate U.S. military capabilities. Such cyber attacks may target military systems specifically, or the civilian critical infrastructure on which civil and military activities depend.

An attack on military systems might result in U.S. guns, missiles, and bombs failing to fire or detonate or being directed against our own troops; or food, water, ammo, and fuel not arriving when or where needed; or the loss of position/navigation ability or other critical warfighter enablers. Moreover, the successful combination of these attacks could severely undermine the credibility of the U.S. military's ability to both protect the homeland and fulfill our extended deterrence commitments.

We have to be confident that we have credible and capable systems to impose costs on adversaries. However, it is not feasible to protect all systems against the full-spectrum capabilities of highly capable actors dedicated to compromising them.

DoD must therefore devote urgent and sustained attention to boosting the cyber resilience of key U.S. strike systems (cyber, nuclear, non-nuclear) – including essential supporting forces and critical infrastructure to ensure we maintain credible response capabilities. **Without such measures, the United States will not be able to effectively deter the most sophisticated large-scale cyber attacks.**

2.1 Establish a Highly Cyber Secure/Resilient "Thin Line" of Strategic Offensive Cyber, Nuclear, and Non-Nuclear Long-Range Strike Capability

Findings:

Scalable military strike capabilities – including offensive cyber, non-nuclear long-range strike, and nuclear systems – are the foundation of U.S. deterrence by cost-imposition. These strike capabilities will be targeted by major powers' cyber (and other) programs, and must both be resilient and perceived as such. For these systems, a perception of vulnerability is dangerous and destabilizing.

In order to avoid presenting an inviting target in crisis, and accelerate escalation rather than support deterrence, it is essential that U.S. strategic offensive cyber capabilities, and at least a sizable fraction of U.S. non-nuclear strike capabilities be highly resilient to cyber attack, and seen as such by U.S. adversaries. If U.S. offensive cyber responses and U.S. non-nuclear strategic strike capabilities are not resilient to cyber attack, the President could face an unnecessarily early decision of nuclear use – assuming that U.S. nuclear capabilities are sufficiently resilient.

Examples of long-range non-nuclear strike systems that should be made highly resilient to cyber (and other non-nuclear attack) on an urgent priority basis include:

- Guided missile submarines (SSGNs) and (particularly as SSGNs are retired) a substantial number of general purpose attack submarines (SSNs) armed with Tomahawk Land Attack Missiles (TLAMs);
- Heavy bombers armed with extended range Joint Air to Surface Standoff Missiles (JASSM-ER) and Massive Ordnance Penetrators (MOPs);
- Supporting command, control, communications and intelligence, surveillance and reconnaissance (C3ISR) essential to support mission planning and execution; and
- Critical infrastructure (CI) essential to support platforms, munitions, C3ISR, logistical support, and personnel.

As the United States recapitalizes new nuclear capabilities, these should not be networked by default. Connectivity may make such capabilities more modern, but also widens their attack surface to adversaries.

Adversaries may attack CI in crisis or conflict in order to: 1) impair the execution of the "Thin Line" missions cited above; 2) attempt to deter or coerce U.S. leadership, e.g., from deploying forces to defend an ally or interest; and 3) attempt to force the United States leaders to divert military forces and capabilities to supporting domestic consequence management through attacks on water systems, the electric power grid and other lifeline

infrastructure. To help the U.S government meet these challenges and get ahead of the intensifying threat, CI owners/operators will need additional cost recovery mechanisms to invest in the resilience of critical infrastructure that support U.S. military capabilities, particularly "Thin Line" strike capabilities as discussed above. Additional information sharing to help regulators understand the imperative for such projects will also be necessary.

Due to the centrality of electrical power generation in supporting military strike capabilities, the cyber security and resilience of electrical power deserves particular attention, and should be supported by increased DoD collaboration with the electric power subsector, the Department of Energy, the Department of Homeland Security, and other key stakeholders in grid resilience.

Recommendations:

- **CJCS, in coordination with USD(P) and Commander U.S. Strategic Command (USSTRATCOM)**: Within three months, propose for Secretary of Defense approval a concept and timeline for establishing a "Thin Line" cyber secure force including specification of specific force elements to be included. Technical and operational approaches (including operational limitations) required for high confidence cyber security should be described – though such approaches should also be expected to evolve over time.
- **Commander USCYBERCOM**: Within three months, develop a comprehensive program of action with milestones for ensuring the cyber security and resilience of specified "Thin Line" U.S. strategic offensive cyber capabilities in the face of determined top tier adversaries. As part of this work, identify and redress essential C3ISR requirements and critical infrastructure dependencies or vulnerabilities. Propose cost-effective means to redress vulnerabilities, and boost resilience.
- **Under Secretary for Acquisition, Technology, and Logistics (USD(AT&L))[13], in coordination with Commander USSTRATCOM, Secretary of the Navy, and Secretary of the Air Force**: Within three months, develop a comprehensive program of action with milestones for ensuring the cyber security and resilience of specified "Thin Line" U.S. nuclear and non-nuclear long-range strike capabilities in the face of determined top tier adversaries. As part of this work, identify and redress essential C3ISR requirements and

[13] The 2017 National Defense Authorization Act, effective February 2018, divides the duties/authorities of the Under Secretary of Defense for Acquisition, Technology, and Logistics into two positions: Under Secretary for Research and Engineering, and Under Secretary for Acquisition and Sustainment. At the time of this report, it has not been determined how the divested duties and authorities will be assigned between these two positions.

CI dependencies/vulnerabilities. Propose cost-effective means to redress vulnerabilities and boost resilience.

- **USD(P) in coordination with USD(AT&L) and CJCS**: Within four months, develop and implement a methodology (including vulnerability analysis and red teaming) to evaluate and enhance the cyber security and resilience of specific offensive cyber, non-nuclear long-range strike, and nuclear strike capabilities; C3ISR and supporting infrastructures should be included.
- **Secretary of Defense**: Immediately require Service Secretaries and Chief of Staffs to develop risk mitigation options for critical infrastructure supporting "Thin Line" offensive cyber and strike capabilities, and report back within four months with prioritized recommendations. Direct particular focus with near-term milestones for power and communication restoration. The Assistant Secretary of Defense for Homeland Defense and Global Security should develop Secretary of Defense guidance to the Services for this work. The key step of mitigation, either by operational measures or technical solutions, must be "owned" by the programs of record and funded/staffed accordingly.
- **USD(P) and USD(AT&L)**: Develop new mechanisms to enable CI owners and operators to recover the costs of investments in critical infrastructure resilience necessary to help DoD mitigate cyber risks to "Thin Line" capabilities, and to help DoD installations ensure they can execute their "Mission Essential Functions." In addition, enhance information sharing to help regulators assess the national security value of resilience initiatives.

2.2 Establish Strategic Cyber Security Program to Drive Sustained Major Improvements in Cyber Resiliency

Findings:

Business as usual will not be adequate to provide a high degree of confidence that systems essential to offensive cyber, long-range strike, and nuclear deterrence are resilient (end-to-end) against top tier cyber attack. A sustained independent red team capability, backed by top-notch analytics and supported by intelligence assessments, is needed. It is vital that such a red team be independent from the mission owner of the system it is evaluating.

This red team should focus on the cyber security of identified strategic cyber, non-nuclear, and nuclear strike systems (and supporting C3ISR and infrastructure). It should address both today's and potential future systems. It should consider all possible forms of cyber attack, including not only remote access, but all others including supply chain operations and insider threats.

The nuclear ballistic missile submarine (SSBN) security program provides a first-cut template for the type of program needed, which includes:

- Emulation of top tier adversaries (Russia and China for cyber).
- Expanded consideration of threats, including both intelligence-based threats, as well as an exploration of technologically possible near-to-long-term threats.
- Informing intelligence collection requirements by establishing hypotheses about adversary approaches.
- Driving a full-range of countermeasures, including concept of operations (CONOPs), system redundancy, requirements, and new technologies.
- Sustaining effort over decades with top-notch leaders and technologically diverse staff.
- Top-cover from the Secretary of Defense.

Recommendation:

- **Secretary of Defense:** Immediately direct the Director of the National Security Agency (NSA) to establish an independent (Strategic Cyber Security Program) SCSP to perform top tier cyber red teaming on offensive cyber, long-range strike, and nuclear deterrent systems. SCSP should look at current systems as well as future acquisitions before DoD invests in or employs new capabilities. SCSP should be formed from top-tier red-teamers and include talent from across the Department of Defense (including reserve component forces and civilians) and the National Laboratories. SCSP findings should be provided to relevant components for action, and the Secretary of Defense should receive quarterly updates on identified challenges, plans, and progress. Because the SCSP will be a small elite organization with a clear focus but limited bandwidth, the Director of NSA should also be directed to establish guidelines for red-teaming and to certify select red teams.

2.3 Establish IT and Operational Technology Security Program for Critical Missions – Nuclear, Non-Nuclear, and Cyber Offense – Increase U.S. Confidence and Adversary Uncertainty

Findings:

A strategic red team that identifies vulnerabilities, as proposed in Section 2.2, is a necessary starting point; however, it must not be an ending point.

The DoD also needs a focused program to ensure best practices are applied in redressing existing and foreseen cyber vulnerabilities. A very wide range of technical approaches is available to enhance security of IT supporting DoD's critical missions. Rather than have each Military Service and Combatant Command devise its own solutions without any communication or synchronization, a central program that captures best practices is needed.

Architected diversity of approaches including redundant systems, "war reserve mode," retro tech (electro-mechanical), diverse supply chain streams, and out-of-band systems could make a substantial difference.[14] Where possible, and without negatively impacting reliability of key systems, advantage can be leveraged in modifying DoD systems at a rate faster than the opposing offense can plan, develop tools, and exploit. This may mean accepting reduced connectivity, and when necessary, delayed timelines, for mission assurance. Some solutions may be too costly to apply to the entire U.S. military – but could and should be applied to key response systems central to cyber deterrence. For example, as the United States recapitalizes new nuclear capabilities, these should not be networked by default. (Connectivity may make such capabilities more modern, but it also widens the attack surface for adversaries.) The United States does not need 100% confidence to provide effective deterrence. Leaders would do well to focus first on minimizing adversary confidence in their ability to disrupt or deny our systems.

In establishing a set of programs to enhance cyber security and resilience of key military and non-military systems, both a sense of priorities and a sense of "how much is enough" are essential. This Task Force has recommended that priority be given to strategic capabilities including select cyber offence, select long-range conventional strike, and all nuclear strike systems. Table 1 below provides the Task Force's recommendation regarding "how much is enough"; much work will be required to meet and sustain the suggested standards.

Recommendation:

- **USD(AT&L)**: Establish a new analytical program to identify the best available or emerging security concepts for critical information systems, drawing best practices and innovative ideas from across DoD and industry. Support urgent deployment of best-of-breed IT security in the end-to-end execution of offensive cyber, long-range non-nuclear strike, and nuclear systems. Increase emphasis and techniques required to protect the supply chain. Ensure SCSP (see recommendation 2.2) evaluates acquisition proposals before DoD invests in and employs new capabilities among the select few strategic strike capabilities that are prioritized.

[14] Military Superiority in an Interconnected World; War on the Rocks; March 9, 2015

Table 1 Setting the Bar for Cyber Resilience to Underwrite Cyber Deterrence

<table>
<tr><th></th><th colspan="4">Cyber Actors of Greatest Concern</th><th></th></tr>
<tr><th>KEY U.S. VULNERABILITIES</th><th>Russia</th><th>China</th><th>North Korea</th><th>Iran</th><th>ISIS / Other Terrorists</th></tr>
<tr><td>Cyber Attack on U.S. Critical Infrastructure</td><td colspan="2">United States cannot avoid significant vulnerabilities to other major powers, but can harden the most vital U.S. critical infrastructure (e.g., electric grid) to increase work factor (and likely ability to attribute) for attacks.</td><td colspan="2">United States cannot accept small states being able to hold vital U.S. critical infrastructure at significant risk. This goal sets the minimal bar for defense and resilience of critical infrastructure.</td><td rowspan="4">United States must prevent any significant cyber attack by these actors</td></tr>
<tr><td>Cyber Attack on Vital U.S. Strike Systems*</td><td colspan="2">Select U.S. strike systems must be highly secure/resilient to underwrite deterrence by cost imposition. This goal sets the minimal bar for resilience of strategic cyber offense, select long-range strike, and nuclear forces and supporting infrastructure.</td><td colspan="2">United States cannot accept small states being able to hold vital U.S. strike systems at risk. May be a “lesser included case” of Russia-China cyber resilience for some systems – but not for strategic offensive cyber.</td></tr>
<tr><td>Cyber Attack on Other U.S. Military Assets*</td><td colspan="2">United States cannot avoid significant disruption to “business as usual” for U.S. military in the event of conflict with major powers.</td><td colspan="2">Unacceptable for small states to be able to significantly affect U.S. military’s ability to deploy and operate globally. This goal sets minimal bar for cyber resilience of U.S. general purpose forces.</td></tr>
<tr><td>“Death by 1,000 Hacks” and Information Campaigns</td><td colspan="4">United States must prevent theft of intellectual property (IP) and establish a pattern of credible responses to impose costs for IP theft and costly cyber intrusions – including intrusions in support of information operations (such as Russia’s 2016 effort to influence U.S. presidential elections).</td></tr>
</table>

2.4 Certify Cyber Resilience of U.S. Nuclear Systems

Findings:

Nuclear forces and supporting infrastructure require sustained and comprehensive assessments of their ability to operate in the face of a major state's cyber attack. Consequently, the Secretary of Defense and the Secretary of Energy submit an annual nuclear stockpile assessment for the President and Congress, attesting to the reliability and performance of U.S. nuclear weapons. Without question, the cyber security and resilience of U.S. nuclear forces (especially nuclear command, control, and communications (NC3)) is of equal and parallel importance.

Recommendations:

- **Secretary of Defense:** Immediately direct Commander USSTRATCOM to conduct an annual assessment of the cyber resilience of the U.S. nuclear deterrent including all essential nuclear "Thin Line" components (e.g., NC3, platforms, delivery systems, and warheads). Commander USSTRATCOM should state his degree of confidence in the mission assurance of the nuclear deterrent against a top tier cyber threat. The assessment should include details of the approach and technical basis of their judgment, as well as recommendations for mitigation. Assessment should be provided with the Commander's comments and recommendations through the CJCS to the Chairman of the Nuclear Weapons Council (NWC) or its successor[15] (currently the USD(AT&L)), and then with any additional comments, to the Secretary of Defense.
- **USD(AT&L)**: As NWC Chairman, oversee immediate establishment of a program of action with milestones to support cyber certification of U.S. nuclear forces and NC3. This certification process must assume concerted adversary attack against nuclear systems based on extensive preparation (e.g., including supply chain, insider threats, and physical sabotage or attack in addition to remote cyber attacks).

[15] The Fiscal Year 2017 National Defense Authorization Act eliminates the position of USD(AT&L), and among other things, currently places the responsibility of chairing the NWC with the newly created Under Secretary of Defense for Acquisition and Sustainment. However, the placement of this responsibility may further evolve in the months ahead as the Secretary of Defense is preparing a plan for devolving USD(AT&L) responsibilities for Congress to review and approve.

3. Enhance Foundational Capabilities

In addition to the measures outlined above, the Department of Defense and the broader U.S. Government must pursue enhancements to several different types of capabilities, each of which is "foundational" in its own way:

- Cyber attribution;
- Cyber resilience of the joint force (to a lesser level than for strategic strike systems, but enhanced relative to today);
- Innovative technologies that can enhance the cyber security of the most vital U.S. critical infrastructure;
- U.S. leadership in providing cyber "extended deterrence" to allies and partners; and
- The sustained recruitment, training, and retention of top-notch cyber cadre.

3.1 Accelerate Improvements in Cyber Attribution Capabilities

Findings:

Attribution is essential for deterrence by cost imposition, and is greatly improved by:

- Improving identification and authentication of the users of our systems;
- Sharing situational awareness between adjacent systems; and
- Conducting behavioral analysis (tying actions to actors), rather than just depending upon transaction analysis (looking principally at tripwire events).

Because advance cyber actors can engage in deception ranging from hiding their tracks to conducting "false flag" operations intended to make it appear that someone else perpetrated an attack, forensic analysis of hacked systems – while essential – will often be insufficient to provide compelling attribution of attacks by the most capable cyber actors. In such cases, the U.S. Government will have to make a very carefully considered choice of whether to declassify intelligence based, for example, on human sources or cyber exploitation. Although such hard choices will never be eliminated, improving both the security of U.S. networks and the art of the possible for forensic analysis can reduce the scope of this challenge over time.

With proper consideration (i.e., not exposing tradecraft or sources) the ability to share information supporting attribution with allies, partners, and the public is essential to maintaining support for actions taken by the U.S. Government. However, the U.S. Government often confuses the private sector regarding the "authoritative" source for

threat information. There is no one, single, authoritative source to obtain actionable threat information to protect and defend the industrial enterprise.

Recommendations:

- **Under Secretary of Defense for Intelligence**: With Joint Staff (J2) and DNI, improve attribution means and methods; increase collection and reporting of foundational intelligence for key adversaries (including people, processes, technology, tools, tradecraft, partners, risk tolerance, etc.); and collaborate with private-sector intelligence and internet security companies to create real-time shared situational awareness across multiple jurisdictions. Within three months, develop processes to establish universally accepted "tear line" protocol to allow for more timely declassification of threat information. Specifically, evaluate and propose to Secretary of Defense and Director of National Intelligence whether the Cyber Threat Intelligence Integration Center should be designated lead for the U.S. Government on attribution.
- **DoD Chief Information Office and Commander USCYBERCOM**: Within three months identify processes and technologies that when applied to our enterprise networks will enhance the probability of attributing penetrations of these systems. Concepts to consider should include: two-factor authentication, out of band logging system, out of band auditing, and behavioral analytics. Implementation of these selected techniques should be expedited. When combined with our increased collection and analysis of foreign actor's cyber capabilities, operations and objectives, we could significantly enhance our ability to attribute attacks to our systems in a timely manner.

3.2 Intensify Efforts to Boost Cyber Resilience of the Total Force

Findings:

Today, both China and Russia are able to cause disruptive attacks against the United States without resorting to highly advanced cyber tools. The low hurdle needed to gain advantage over our defenses likely increases their confidence in their ability to coerce or deter the United States by exploiting vulnerabilities in ICT and ICS in order to hold our civilian and military critical infrastructure and systems at risk.

Although the United States cannot avoid significant cyber disruptions to U.S. military systems in the event of a conflict with major powers (e.g., Russia and China), boosting the resilience of U.S. General Purpose Forces (GPF) can provide a backstop to deterrence of these actors in two essential ways. First, the breadth and diversity of U.S. GPF provides a source of potential response capabilities to an all-out top tier attack, and therefore a hedge and boost to highly cyber-protected strike forces. Second, continued improvement of GPF

cyber resilience provides a "moving target" – so adversaries cannot focus all attention and resources on subverting highly cyber-protected strike forces.

It is unacceptable for second tier actors to be able to significantly affect U.S. military's ability to deploy and operate globally. Getting ahead and staying ahead of small state threats sets the bar for the cyber resilience of U.S. GPF.

Recommendations:

- **CJCS:** Sustain focus on continued improvement in cyber resilience for U.S. GPF, including requiring CCMDs to plan and exercise to operate in cyber degraded environments. Ensure Global Combatant Commands (GCCs) understand their reliance upon international partner critical infrastructure, and help build partner capacity for resilience of this infrastructure. Facilitate cooperation between U.S. Transportation Command and GCCs to understand impacts and workarounds in the event of cyber degradation of troop and logistics movements.
- **Service Secretaries and Director of Operational Test and Evaluation:** Continue to focus on developmental testing and operational testing in realistic cyber adversary environments, systematically raising the bar over time.
- **Vice Chairman of Joint Chiefs of Staff and USD(AT&L):** Ensure appropriate weighting is given to cyber security/resilience during the requirements and acquisition processes. Develop a program to infuse strong cybersecurity and software development expertise into the acquisition process.

3.3 Act as Innovative Accelerator to U.S. Governmental Efforts to Boost Cyber Resilience of Critical Infrastructure

Findings:

Lesser powers (particularly Iran and North Korea), and potentially non-state actors including ISIS, have a limited but potentially increasing ability through cyber tools—indigenous, purchased, or transferred—to conduct catastrophic attacks on U.S. critical infrastructure. The dependence of the United States on modern ICT and ICS to facilitate every aspect of our lives – to operate the government, all of our critical infrastructures (e.g., energy, water, and financial sectors), and our general business and citizen enterprises – has made these systems attractive targets to a wide spectrum of adversaries.

Virtually any actor with substantial resources can now develop or buy the capability to attack elements of U.S. critical infrastructure with cyber weapons. North Korea, Iran, and terrorist groups have strong motivation to purchase such capabilities where possible, and to develop their own substantially improved attack capabilities.

It is essential to U.S. security, and U.S. credibility on the world stage, that such lesser state powers or terrorist groups not be allowed to pose a strategic threat to U.S. critical infrastructure, or to be able to significantly affect the U.S. military's ability to deploy and operate globally. Thus, deterrence by denial (buttressed by deterrence by cost imposition) must be the foundation of U.S. cyber deterrence for these actors.

Recommendations:

- **USD(AT&L)**: With the "Thin Line" cyber resilient force as first priority, spur and evaluate innovative technologies aimed at breakthrough improvements in cyber security and the cyber resilience of the U.S. military. The relevant technologies should then be carefully shared with owners of critical infrastructure, through existing interagency processes. Cyber-resilient electrical power, water, waste-water and communications systems should be particular priorities.

3.4 Additional Issues

Findings:

The DSB Cyber Deterrence Task Force identified two critically important areas where additional work by the DoD and U.S. Government is needed: cyber extended deterrence, and ensuring a top-notch cyber cadre.

Recommendations:

- **USD(P)**: In order to accelerate efforts to backstop **extended deterrence** and boost allied/partner cyber security, develop guidance for Secretary of Defense and Presidential approval on appropriate U.S. cyber commitments. Also, continue to build and implement game-plans for assisting key ally or partner cyber security, and additionally develop guidelines associated with responding to requests for offensive cyber capabilities. Provide direction to CCMDs for related engagement. Work with Joint Staff and Commander USCYBERCOM to normalize processes for Cyber Mission Force teams to conduct technical exchanges and joint cybersecurity missions with international partners.
- **Commander USCYBERCOM**: In order to accelerate development of a **top-notch cyber cadre**, USCYBERCOM and each of the Services should develop a talent management plan/strategy for their offensive and defensive cyber forces (including red teams). In order to ensure long-term cyber analytic cadre focus that develops deep expertise, take documented steps to ensure that cyber intelligence ranks long-term target familiarity and expertise as among the top personnel assignment requirements.

Appendix 1: Task Force Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION, TECHNOLOGY AND LOGISTICS

OCT 0 9 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber Deterrence

The objective of the Cyber Deterrence Task Force is to consider the requirements for effective deterrence of cyber attack against the United States and U.S. allies/partners, and to identify critical capabilities (cyber and non-cyber) needed to support deterrence, war-fighting, and escalation control against a highly cyber-capable adversary.

The task force should consider alternative adversary concepts for cyber attack, ranging from a sustained "under the radar" campaign designed to impose costs, to gradual escalation, to rapid large-scale cyber attack at the outset of a broader campaign. The task force should describe policy, operational, and technological elements of an effective deterrence and response posture, to include: declaratory policy; methods for determining whether a cyber attack (versus cyber exploitation) is occurring; means for rapid high-confidence attribution of attack; approaches to reducing any challenges of sharing attack assessment data with allies/partners; potential thresholds for various military and non-military responses and how these thresholds should be communicated to allies/partners and potential adversaries; what types of military response capabilities could best help deter attack, and ensure that the United States and its allies/partners have adequate capabilities in the event of conflict; whether enhanced levels of cyber protection should be pursued for select elements of the joint force in order to ensure these elements of the force would be available for use in the immediate aftermath of a major cyber attack; what military capabilities may be most important to support operations against a highly cyber-capable foe; the potential contribution to deterrence and war-fighting of increased resilience of critical DoD and non-DoD infrastructures as well as the ability to operate in a "cyber-degraded" environment; and approaches for rapidly assessing and weighing the risks of action versus the risks of inaction in various scenarios.

I will sponsor the study. Mr. James R. Gosler and The Honorable James N. Miller, Ph.D., will serve as Co-chairmen. Jonathan Reiber, OUSD(Policy), will serve as Executive Secretary. Lt Col Michael Harvey, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

THIS PAGE LEFT INTENTIONALLY BLANK

Appendix 2: Task Force Membership

Co-Chairs

Mr. James Gosler
Senior Fellow, Johns Hopkins University Applied Physics Laboratory

Honorable James N. Miller
President, Adaptive Strategies, LLC

Members

Mr. Robert Butler
Co-Founder and Managing Director, Cyber Strategies LLC

General Michael Carns, U.S. Air Force, (Retired)
Private Consultant

Ms. Melissa Hathaway
Private Consultant

Dr. Robert Hermann
Private Consultant

Mr. Jason Healey
Columbia University's School of International and Public Affairs and Senior Fellow, Atlantic Council

Mr. John (Chris) Inglis
Visiting Professor of Cyber Studies at the U.S. Naval Academy

Dr. Martin Libicki
Private Consultant

Dr. Joseph Markowitz
Private Consultant

Honorable Judith Miller
Private Consultant

Honorable Arthur Money
Private Consultant

Admiral Eric T. Olson, U.S. Navy (Retired)
President, ETO Group, LLC
Former Commander, U.S. Special Operations Command

General Norton Schwartz, U.S. Air Force, (Retired)
President/CEO, Business Executives for National Security

Honorable Paul Stockton
Managing Director, Sonecon, LLC

Executive Secretary

Ms. Katherine Charlet
OUSD(Policy)

Mr. Jonathan Reiber
OUSD(Policy)

Senior Reviewer

Honorable William LaPlante
Mitre Corporation

Defense Science Board Secretariat

Ms. Karen Saunders
Executive Director

Mr. Dave Jakubek
DSB, Former Executive Director

Col Robert Freeland
DSB, Former Executive Director

Lt. Col. Victor Osweiler
DSB Military Representative

Support Staff

Mr. Chris Grisafe
SAIC

Ms. Kathleen McGlynn
SAIC

Appendix 3: Briefings Received

Remarks and Discussion
Hon. Eric Rosenbach, Assistant Secretary of Defense for Homeland Defense and Global Security

FBI Cyber Briefing
Mr. James C. Trainor, Federal Bureau of Investigations

CIA Cyber Briefing
Mr. Tom Donahue, Central Intelligence Agency

U.S. Cyber Command Briefing
Admiral Michael Rogers, USCYBERCOM

Joint Chiefs of Staff Briefing
Admiral James "Sandy" Winnefeld, Joint Chiefs of Staff

White House Cyber Briefing
Hon. Michael Daniel, White House

Presentations and Discussions
Ms. Leigh Warner; Mr. Rich Haver; Admiral Bill Studeman (USN, Ret.), Private Consultants

CNCI Deterrence and Global Observations
Ms. Melissa Hathaway, Task Force Member

Bits and Bites of Deterrence
Hon. Richard J. Danzig

Cyber Deterrence to Protect Critical Infrastructure, Intellectual Property, and Address Cyber Fraud
Ambassador Joseph DeTrani

Presentation and Discussion
Mr. Sean Kirkpatrick

Cyber Risk Assessment
Mr. Chuck Nicholson, U.S. Strategic Command

Defense Innovation Initiative
Dr. Ron Jost; Mr. Adam Nucci, Department of Defense

CrowdStrike
Mr. Dmitri Alperovitch

Information and Cyber Security
Mr. Phil Venables

VTC Presentation and Discussion
Mr. Greg Rattray, JP Morgan Chase

Cyber Deterrence
MG Paul Nakasone, National Security Agency

ICS-CERT Coordination
Ms. Monica Maher; Mr. Mark Bristow, Department of Homeland Security

Deterrence Doctrine and Threats
Mr. Hank Messick; Mr. Mike Torrey; Mr. Joseph Cheravitch; Mr. Ronald Draker

Presentation and Discussion
Mr. Fred Ruonavar; Mr. Will Schmittt

Turbulent Winter
Mr. Bob Butler

Big Ideas for Findings and Recommendations
Dr. Paul Stockton, Managing Director, Sonecon, LLC

SPR Update
Lt Gen Robert E. Schmidle, Deputy Director, Cost Assessment and Program Evaluation, Department of Defense

Cyber Security in a "Brave New World"
Mr. Terry Boston, CEO of PJM

Technology Update
Ms. Leigh Warner

End Game
Mr. Nate Fick

Cyber Awakening
CAPT Mike Elliott, U.S. Navy

"Operation Gimble Ruckus"
CDR Kallie Fink; CDR Paul Lashmet

Technology Panel Discussion
Ms. Leigh Warner; Mr. Neal Ziring; Dr. Chris Locke; Dr. Boyd Livingston; Mr. Ryan Agee; Dr. Yul Williams; Dr. Thomas Walcott; Mr. Steve Ryan

Capability Development Then – Panel Discussion: Cyber Roots
Mr. Bill Black; ADM Bill Studeman; Mr. Rich Haver

Cybersecurity Scorecard – Culture and Compliance Initiative
Mr. Richard Hale, Deputy Chief Information Officer, Department of Defense

IC Briefing: Capabilities and Use Doctrine
Regional Experts

Continuity of Operations – USAA Security and Resiliency
Mr. Dave McDermitt

Capability Development Now – CMF Equip Model
Col Dean "Data" Clothier

Capability Development Then – Panel Discussion: Cyber Roots
Mr. Bill Black; ADM Bill Studeman; Mr. Rich Haver

Cybersecurity Scorecard – Culture and Compliance Initiative
Mr. Richard Hale

Follow-Up Discussion
Hon. Richard Danzig

Resiliency Activities and Policy Issues
Mr. Scott Aaronson; Mr. David Batz

Continuity of Operations – Telco: AT&T
Mr. Ed Amoroso; Mr. John Nagengast

Strategic Deterrence
CAPT Brent Sadler, USN

Appendix 4: Acronyms

C3	Command, control, and communications
C3ISR	Command, control, communications, intelligence, surveillance, and reconnaissance
CCMD	Combatant Command
CI	critical infrastructure
CJCS	Chairman of the Joint Chiefs of Staff
CONOP	Concept of operations
DDoS	Distributed Denial-of-Service Attack
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DSB	Defense Science Board
GPF	General Purpose Forces
IC	Intelligence Community
ICS	Industrial control system
ICT	Information and communications technology
IP	Intellectual property
ISIS	Islamic State of Iraq and Syria
IT	Information technology
J2	Joint Staff Intelligence Directorate (or of a military staff)
JASSM-ER	Extended Range Joint Air-to-Surface Standoff Missile
MOP	Massive Ordnance Penetrator
NC3	Nuclear Command, Control, and Communications

OUSD(P)	Office of the Secretary of Defense for Policy
SCSP	Strategic Cyber Security Program
SECDEF	Secretary of Defense
SSBN	Ship, Submersible, Ballistic, Nuclear (ballistic missile submarine)
SSGN	Ship, Submersible, Guided Missile, Nuclear (guided missile submarine)
TLAM	Tomahawk land-attack missile
USCYBERCOM	United States Cyber Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USG	United States Government