Statement

By

Dr. Craig Fields
Chairman, Defense Science Board

And

Dr. Jim Miller
Member, Defense Science Board
Former Under Secretary of Defense (Policy)

Before the

Armed Services Committee, United States Senate

Cyber Deterrence

March 2, 2017

Introduction

Chairman McCain, Ranking Member Reed, Members of the Committee. We are here today to discuss cyber deterrence.

By "cyber deterrence" we mean how to deter major cyber attacks on the United States, largely by foreign states, particularly great powers, but someday perhaps by capable non-states.

We want to begin by briefly introducing the Defense Science Board (DSB) and telling you about DSB's substantial agenda of studies regarding cyber. Then I have some fundamental principles to offer regarding how to be successful with cyber deterrence.

We will then turn to Jim Miller, co-chair with Jim Gosler of DSB's recent comprehensive study of cyber deterrence. He will present the major findings and recommendations of that investigation.

We would also like to underscore that the findings we reference are the Defense Science Board's and do not necessarily represent the perspectives, policies, or positions of the Department of Defense.

Defense Science Board

For 60 years the Defense Science Board (DSB) has tackled highly unstructured, irksome and consequential problems for the Secretary of Defense that involve science and technology. And, inevitably, also strategy, tactics, management, rules of engagement and operational concepts as related to science and technology.

The members of DSB are senior executives from defense and commercial industry; retired flag officers; former senior officials from the Department of Defense, Department of State and the Intelligence Community; University professors, e.g. from MIT; CEOs of Federally Funded Research and Development Centers; National Laboratory Directors; and many members of the National Academy of Science and the National Academy of Engineering.

All with a strong background in science and technology; and with knowledge of DoD and national security matters.

Defense Science Board Studies on Cyber

DSB's first study on cyber dates from 1967, and to my knowledge that work was the first major investigation of the cyber threat with recommendations regarding how to mitigate and manage the threat.

Much more recently DSB has conducted a series of studies that in union provide a comprehensive set of findings and recommendations for the Department of Defense.

Cyber Resilience –- recommendations for defense against low- and medium-level threats, and the recognition that we cannot adequately defend against high-level threats. Those must be deterred.

Cyber and Cloud Computing –- How can DoD realize the tremendous benefits of economy of scale of cloud computing, while mitigating the risks of such shared and remote computing?

Cyber Defense Management –- Insofar as cyber defense can be expensive – noting that lack of cyber defense can be considerably more expensive! – how should DoD optimally allocate its resources to provide the best protection?

Cyber Corruption of the Supply Chain – How can DoD mitigate the risk of malicious insertions in the microelectronics it buys?

Cyber Offense as a Strategic Capability – What does DoD have to do to ensure that the President has strategic options at hand to use prudently as unpredicted needs arise?

Acquisition of Software -- In general how can DoD acquire software better, and in particular how can DoD mitigate the risk of cyber intrusion into our software?

21st Century Multi-Domain Integration – harmonizing cyber, kinetics and EW in all domains, in terms of capabilities, planning, training, C3 and so on

Cyber Deterrence – What needs to be done to effectively deter major cyber attacks on the United States?

In addition, cyber considerations play a role in almost all DSB studies. Most DoD systems contain computing, and most computing is vulnerable to cyber.

Thus, cyber considerations play a role in many DSB studies, including: information operations in gray zone conflicts; unmanned undersea vehicles; autonomous systems; countering autonomous systems; survivable logistics; electronic warfare (EW); ballistic and cruise missile defense; MILSAT and tactical communications; resilience of space capabilities; air dominance; and more.

Some Fundamental Principles of Cyber Deterrence

I would like to offer eight (8) fundamental principles that apply to cyber deterrence. The principles do NOT dictate exactly what to do in particular circumstances, but what to do in particular circumstances should conform to the principles.

First, we must deter specific people, specific individuals, the decision makers of foreign states, not countries. They decide whether or not to unleash a cyber attack on the United States. Trying to deter lower level individuals, e.g. 22-year-old hackers, mid-career civil servants, lower level military officers who are "following orders" is not effective.

Second, deterrence of an individual is an exercise in psychology, not physics. Physics is easier. It is an exercise in cross-cultural psychology, to make it more difficult. It is an exercise in situation-dependent psychology to make it more difficult still. Finally it is an exercise in psychology done from a distance insofar as the U.S. Government personnel charged with deterrence will likely have never met the individual we want to deter, or certainly have not spent sufficient time with them to develop deep understanding. That's the way it is. The implication is that we have to do the best we can, meaning be sure that the U.S. Government personnel charged with cyber deterrence have access to the very best analysis regarding the individuals we want to deter.

Third, to deter a leader who might decide to order a cyber attack on the U.S. we need to hold at risk what they hold dear. We have to make their expected cost greater than their expected benefit. Where feasible at reasonable cost we should also decrease their expected benefit of a cyber attack on the U.S., e.g. with defense, protection, resilience or reconstitution of our critical infrastructure, but for the most capable adversaries, e.g. great powers, that is difficult.

Fourth, cyber deterrence does not have to be 'like for like', 'tit for tat'. Cyber does not have to be deterred with cyber. Deterrence could involve economic sanctions or other means.

Fifth, and related, U.S. responses to cyber attack do not have to aim to impose (only) a similar level of costs on the adversary as it imposed on the United States. While a response must meet legal requirements such as proportionality (avoiding unnecessary civilian loss of life or hardship), it must also be effective. That means imposing sufficient costs to deter future such attacks.

Sixth, escalation is always a concern and should always be a concern. All deterrence is accompanied by the *possibility* of escalation. But lack of deterrence is accompanied by the *certainty* of escalation. We are often faced with the alternatives of a *certainty* of 'a death of a thousand cuts' if we take no deterring action or the *possibility* of escalation if we take deterring action. There is no perfect solution but there is a constructive approach, namely to employ approaches to deterrence that are graded – do a little, see what happens, do a little more… -- and reversible.

Seventh, chronology. It is considerably more effective to take deterring action sooner rather than later. Being prepared to act sooner carries some operational implications. Long in advance the Intelligence Community has to be tasked to collect the underlying information required to compose strategy, tactics and operational

plans for deterring specific individuals. Long in advance the organizations that would be tasked with affecting deterrence, e.g. DoD, Treasury, need to have capabilities prepared and in place and compose the aforementioned strategy, tactics and operational concepts. And all this has to be orchestrated across various organs of the Executive Branch with effective communication with the appropriate elements of the Congress.

Eighth, credibility is a necessary enabler of deterrence. If the leader we want to deter does not believe we will act it is difficult to deter. Announcing 'red lines' and then overlooking offenses is not constructive.

To repeat, these eight principles do not dictate specific deterring actions for particular circumstances, but if we want to be effective in deterring major cyber attacks on the U.S. we should comply with the principles.

Defense Science Board Study of Cyber Deterrence

The DSB Cyber Deterrence Task Force was asked to consider the requirements for deterring 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 highly cyber-capable adversaries. In conducting its work, the fifteen task force members received more than forty briefings from government, the national laboratories, academia, and the private sector.

Three Key Cyber Deterrence Challenges

The task force determined that the United States faces three distinct sets of cyber deterrence challenges.

First, **m*ajor powers (Russia and China)*** *have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack – and to simultaneously use cyber to undermine U.S. military responses.* The unfortunate reality is that for at least the next decade, the offensive cyber capabilities of these major powers are likely to far exceed the United States' ability to defend essential critical infrastructure. At the same time, they *recognize that the U.S. military itself has an extensive dependence on information technology, and they are pursuing the capability to use cyber to thwart U.S. military responses. This emerging situation threatens to place the United States in an untenable strategic position.*

Second, ***regional powers (such as 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. The United States would have a range of options to respond to any attack (cyber or

other) by such nations. But these response capabilities must be additive to our defenses. 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 three challenges, bolstering the U.S. cyber deterrence posture must be an urgent priority. The task force recommended that the Department of Defense and broader U.S. government pursue three broad sets of initiatives.

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 – including Russia, China, Iran, North Korea, and non-state actors including ISIS. 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.

This requires, and the task force recommended:

- **Updated declaratory policy** that makes clear the United States will respond to all cyber attacks; the question will not be whether but how.

- **Cyber deterrence campaign plans** focused on the leadership of each potential adversary.

- **Adversary-specific "playbooks"** of response options to cyber attacks 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.

- **Specific offensive cyber capabilities** to support approved "playbook" options by holding at risk what is valued by adversary leaders; this should include capabilities that do not require "burning" intelligence accesses (sources and methods) when exercised.

- **An offensive cyber capability tiger team** to develop options to accelerate acquisition of offensive cyber capabilities to support deterrence, such as additional acquisition authorities for USCYBERCOM, and establishment of a small elite rapid acquisition organization.

The intention is not to create a "cookbook" approach to cyber deterrence. Rather it is to establish a clear policy and planning framework, to help drive prioritized cyber offensive capability development, and ultimately to give a range of good cyber and non-cyber options to support deterrence of – and as necessary response to – cyber attack.

2. *Create a Cyber-Resilient "Thin Line" of Key U.S. Strike Systems*

In order to support deterrence, the United States must be able to credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks. Meeting this requirement will require the Department of Defense to devote urgent and sustained *attention* to boosting the cyber resilience of select U.S. strike systems (cyber, nuclear, and non-nuclear) including their supporting critical infrastructures. 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.

This requires a **"thin line" cyber secure force** comprised of select elements of offensive cyber capabilities, select non-nuclear long-range strike systems, and all nuclear-capable systems. The Department should further enhance investments to protect and make resilient these capabilities. Examples of long-range non-nuclear strike systems that should be made highly resilient to cyber (and other non-nuclear attack) on an urgent basis include:

- A substantial number of general purpose attack submarines (SSNs) and guided missile submarines (SSGNs) armed with long-range strike systems (for example Tomahawk Land Attack Missiles (TLAMs));
- Heavy bombers armed with non-nuclear munitions capable of holding at risk a range of targets in standoff or penetrating mode (for example, 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 essential to support platforms, munitions, C3ISR, logistical support, and personnel.

In support of this "thin line" cyber secure force, the task force recommended:

- **An independent Strategic Cyber Security Program (SCSP)** housed at the National Security Agency (NSA) to perform top tier cyber red teaming on selected 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. The Navy's long-standing SSBN Security Program provides a useful model.

- **A new "best of breed" cyber resilience 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. This program should devise a broad portfolio of options to dramatically enhance cyber resilience of critical strike systems, ranging from emerging new technologies to the use of "retro-tech" such as electro-mechanical switches.

- **An annual assessment of the cyber resilience of the U.S. nuclear deterrent**, conducted by the Commander of U.S. Strategic Command, and provided to the Secretary of Defense, President, and Congressional leadership. including all essential nuclear "Thin Line" components (e.g., nuclear C3, 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.

3. Pursue Foundational Capabilities

In addition to the measures outlined above, the Department of Defense and the broader U.S. Government must continue to innovate in order to improve the posture of the United States regarding several foundational capabilities:

- **Cyber attribution**;

- **Continued enhancement of cyber resilience of the joint force** – though to a lesser level and as a lower priority than for selected long-range strike systems as discussed above;

- **Offensive and Defensive Cyber Security S&T**: U.S. research in both of these areas need to inform the other;

- **Innovative technologies** that can enhance the cyber security of the most vital U.S. critical infrastructure;

- **U.S. leadership in providing appropriate cyber "extended deterrence"** to allies and partners; and over time perhaps most importantly,

- **The sustained recruitment, training, and retention of a top-notch cyber cadre**.

Over the last several years, the Department of Defense has begun taking important steps to strengthen its cyber capabilities, including for example the establishment and initial operating capability of 133 cyber mission force teams. If implemented and sustained over time, the task force recommendations (outlined in this statement and described in much greater detail in the DSB report) will build from this prior

work, and help guide the urgent actions needed to bolster deterrence of cyber attacks on the United States and our allies and partners.