A Blueprint for Cyber Deterrence: Building Stability through Strength

Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi

> "In many ways, deterrence in cyberspace is eminently more complicated than deterrence in the Cold War. The nature of the domain makes it so. Even the most sophisticated theories behind nuclear deterrence will prove inadequate for dealing with the complexities of a man-made domain with a virtually infinite number of constantly changing actors, motivations, and capabilities."[1]

Cyber threats pose a real and growing problem, and to date, United States efforts to counter them have lagged. While the ability to defend against an attack or intrusion must be maintained, the US, like any country, would be well served by deterring its adversaries from acting in the first place – at least when it comes to the most serious of actions, namely cyber warfare. Clearly not all hostile behavior can be deterred, but it is important to identify priorities in this regard and determine how best to address those that lead the list. Despite animated discussions, development of a grand unified solution has remained elusive, in part because the complexity and crosscutting nature of cyber deterrence requires a comprehensive and cohesive solution that encompasses stakeholders in both the private and public sectors.

Frank J. Cilluffo is director of the George Washington University Homeland Security Policy Institute (HSPI) and co-director of GW's Cyber Center for National & Economic Security (CCNES). Sharon L. Cardash is associate director of HSPI and a member of CCNES. George C. Salmoiraghi is an attorney and advisor to HSPI in Washington, D.C.

In order to help structure the debate and advance toward the goal, we propose a framework that examines the issue critically and looks to dissuade, deter, and compel both state and non-state hostile actors. Placing potential threats into conceptual relief this way helps clarify the sources of danger and serves as a starting point for determining and attaching responsibility for hostile action(s) against a country or its allies. This then allows the relevant players who have been targeted by hostile actors to proceed with necessary discussions and action as both a precursor to, and actual execution of, appropriate and effective response measures. The rubric thus yields a further corollary benefit by aiding to identify areas that would benefit from or even require cooperation among affected/targeted entities. In short, this framework provides a starting point to explore ways to deter hostile actors, and as such offers a conceptual lens that can be of value to the US and its allies alike. Neither the range of actors nor their potential activities detailed below is meant to be exhaustive. It is instead a snapshot, and a rough one at that, intended to help convey a sense of who, what, how, why, and so on, as a prelude to a more in-depth discussion of strategy and policy in the area of cyber deterrence.

State Actors

Foreign militaries may engage in computer network attack/computer network exploitation (CNA/CNE) to limit, degrade, or destroy another country's abilities, in furtherance of a political agenda. Foreign militaries are increasingly integrating CNA and CNE capabilities into their war fighting and military planning and doctrine.[2] Such efforts have conventional battlefield applications (i.e., enhancing one's own weapon systems and platforms, and/or stymieing those of others); and unconventional applications, as cyberspace extends the battlefield to incorporate broader civilian and societal elements. Cyber domain activity may cover intelligence preparation of the battlefield, to include the mapping of critical infrastructures of perceived adversaries.[3]

Foreign intelligence and security services: Exploits may include political, military, economic, and industrial espionage; theft of information from or about another government; or theft of intellectual property, technology, trade secrets, and so on in the hands of private corporations and universities. Many foreign intelligence services are engaged in industrial espionage in support of private companies.[4] Ultimate aims of activities

by this actor category include the desire to influence decisions, and affect the balance of power (regionally, internationally, and so on). Convergence of human and technical intelligence is especially notable in this category, and includes the "insider" threat.[5]

Hybrid aspects: Elements of state capability may be integrated to achieve a whole that is greater than the sum of its parts. Alliances (state-to-state) may be invoked for a similar effect. Joint activity in this respect may include collection of information, sharing of findings obtained by a single party, and joint execution of field operations (attacks). States may also seek and enlist the assistance of non-state actors, such as hackers for hire who do not feel bound or restricted by allegiances.

Non-State Actors

Non-state terrorist organizations may conduct CNA/CNE in furtherance of a specific political agenda. They place high value on the internet (to recruit, train, fundraise, plan operations, and so on).[6] US and allied counterterrorism efforts yielding success in the physical world may lead al-Qaeda and their ilk to enter the cyber domain ever more deeply. The latter might try to learn lessons from (or even "surf" in the wake of) the actions of "Anonymous" and other "hacktivists" who use the cyber domain to bring attention to the cause they espouse.

Non-state criminal enterprises, which include theft of intellectual property, identity, and the like, as well as fraud, are generally motivated by profit. Cyber-specific tools and techniques can yield major monetary rewards. The global cybercrime market was valued at $12.5 billion-plus in 2011,[7] though estimates vary (validity of calculation methodologies and impartiality of certain sources is debated and empirical evidence is difficult to obtain).

Hybrid aspects: Alliances of convenience are possible among non-state actors (terrorist and criminal groups, and even individuals) to fill capability gaps, generate force multiplier effects, and so on. Similar arrangements of mutual convenience are also possible between state and non-state (terrorist, criminal, lone hacker) entities; a non-state actor serves to expand a state's skills and capabilities, or acts as a state's proxy for other purposes. Such arrangements further compound the attribution challenge (who is responsible) and provide for additional plausible deniability.

Against deterrence in the nuclear realm,[8] the cyber counterpart bears both similarities and differences.[9] The cyber domain in particular

demands a focus on actors, rather than weapons/capabilities alone; hence prioritizing these actors according to the scope, scale, and nature of the threat that they pose is critical. Only after racking and stacking them can we focus on the actors that matter most, and do so in a way that confronts and neutralizes their specific intentions and capabilities.

Defense and offense are both crucial components of a multilayered and robust US posture and strategy designed to ensure national safety. Deterrence can provide an additional layer of protection by preventing those with interests inimical to the United States from leaving the starting blocks. To preserve as well as further national/homeland security, it is therefore important to think through, develop, and sustain over time in a quickly evolving (technological and security/defense) ecosystem the requisite US capabilities and capacities to support the country, credibly and effectively, in standing ready and being able to dissuade, deter, and compel its adversaries. While concerted efforts directed toward these ends should be pursued in parallel with committed efforts to defend systems, such an approach and stance must not be taken as a substitute for building and maintaining strong additional means of reconstitution that give rise to strong resilience. Indeed, resilience itself may be a powerful deterrent. Reflecting the wisdom of Sun Tzu, the capacity to bounce back after an incident plus the demonstrated will and ability to respond to a cyber attack should serve to strengthen US deterrence efforts and thereby avoid battle and bloodshed: "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[10]

Contours of the Cyber Threat

The United States and its interests are under daily cyber threat from both state and non-state actors. Potential US targets are many and varied, and extend to critical sectors such as water, power, finance, and telecommunications.[11] According to press reports citing a spokesman for the National Nuclear Security Administration, the US "Nuclear Security Enterprise experiences up to ten million 'security significant...events' each day."[12] Tallies of the Department of Homeland Security reveal tens of thousands of cyber intrusions (actual/attempted) each year, and dozens of attacks on critical infrastructure systems – the latter total increasing by several orders of magnitude from 2010 to 2012.[13] The range of senior

officials, past and present, who have sounded the alarm bell is striking, and includes Assistant to the President for Homeland Security and Counterterrorism John O. Brennan;[14] Director of the National Security Agency and Commander of US Cyber Command General Keith Alexander; former Homeland Security Secretary Michael Chertoff; former National Coordinator for Security and Counterterrorism, and former Special Advisor to the President for Cyber Security, Richard Clarke; the Chairman of the Senate Homeland Security Committee, Senator Joseph Lieberman;[15] ranking member on the Senate Armed Services Committee, Senator John McCain; and FBI Director Robert Mueller, who recently predicted that the cyber threat will in the future displace terrorism as the top threat to the country.[16]

One commentator noted vividly, "Foreign spies and organized criminals are inside of virtually every U.S. company's network. The government's top cybersecurity advisors widely agree that cyber criminals or terrorists have the capability to take down the country's critical financial, energy or communications infrastructure."[17] Yet in addition to suffering monetary losses that the Office of the National Counterintelligence Executive and other US officials number in the billions due to computer network exploitation in the form of backdoor theft of valuable intellectual property,[18] the country is taking a more ominous hit as the subject of adversarial efforts to engage in the cyber equivalent of intelligence preparation of the battlefield – including China's mapping of critical US energy and water supply infrastructures, which could later be leveraged so as to deter, dissuade, or compel action on the part of the United States.[19]

Critical industries in other countries have experienced cyber attacks. Saudi Aramco (state owned and "the world's biggest oil producer") saw a virus of external origin infect roughly 30,000 of its computers in August 2012.[20] Shortly thereafter Qatar's RasGas ("the second largest producer of liquified natural gas in the world") was also hit.[21] Newspaper reports suggest that the "French nuclear power group Areva was the target of a cyber attack in September [2011]."[22] And the list goes on.

While countries possess abilities of varying degrees and sophistication, dozens are expanding their cyber capabilities, including the United States and its allies (Israel is a prime player in this domain). Vis-à-vis the United States, China is a key source of "advanced persistent threats," though state sponsored fingerprints are not always evident on the mouse or touch screen.

Attribution is all the harder when there is a substantial delay between the event and the victim's report or request for assistance.[23] Evidence of Chinese intent, though, has existed for more than a decade: in 1999, two Chinese army colonels published a book titled *Unrestricted Warfare*, which highlighted alternative means to defeat an opponent, distinct from traditional direct military action.[24]

Russia too is a sophisticated and determined adversary in the cyber domain. In the 2008 conflict between Russia and Georgia, Russia attacked and disrupted Georgia's communications network. As Ambassador David Smith observes, "Russia has integrated cyber operations into its military doctrine"; though "not fully successful...Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine... [and] we must assume that the Russian military has studied the lessons learned."[25] In 2007, Estonia's government, banks, and other entities were also the target of "large and sustained distributed denial-of-service attacks (DDoS attacks)...many of which came from Russia."[26] Hackers and criminals based in Russia have made their mark. Cyberspace has proven to be a gold mine for criminals, who have moved ever more deeply into the domain as opportunities to profit there continue to multiply. The value of the global cybercrime market in 2011 has been pegged at over $12.5 billion, with Russia's slice of the pie being $2.3 billion (close to double of its absolute value compared to the prior year). There are indications, moreover, that the forces of organized crime in the country have begun to join up "by sharing data and tools" to increase their take.[27]

The potential for cooperation between and among actors with substantially different motivations is of serious concern. For instance, states that lack indigenous capabilities but wish to do harm to the United States or its allies may co-opt or simply buy/rent the services and skills of criminals and hackers to help design and execute cyber attacks. Do-it-yourself code kits for exploiting known vulnerabilities are easy to find, and even the Conficker worm (variants of which still lurk, forming a botnet of approximately 1.7 million computers) was rented out for use.[28] Thus, lack of access to the infrastructure or backing of a powerful state is not prohibitive. Proxies for cyber capabilities are available. There exists an arms bazaar of cyber weapons. Adversaries do not need capabilities, just intent and cash.[29] This is a chilling prospect, bearing in mind that al-Qaeda has called for electronic mujahidin to attack the US government and

critical US infrastructure. Rear Admiral Samuel Cox at Cyber Command noted that al-Qaeda operatives are actively pursuing the means to attack US networks, a capability that they could buy from criminal hackers.[30] In addition, cyber capabilities (however acquired) may be used as a force multiplier in a conventional attack.

Other notable actors of concern in this context include North Korea and Iran. What both of those countries may currently lack in capability they make up for in abundance of intent. Iran is investing heavily to expand and deepen its cyber warfare capacities.[31] The country has also long relied on proxies such as Hizbollah, which now boasts a companion organization called Cyber Hizbollah, to strike at perceived adversaries. Law enforcement officials note that Cyber Hizbollah's goals and objectives include training and mobilizing pro-regime (meaning pro-government of Iran) activists in cyberspace. In turn and in part, this involves schooling others in the tactics of cyber warfare. Hizbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. Each such exploit generates additional opportunities to gather yet more data, as new potential targets are identified, and tailored methods and means of approaching them are developed.[32]

In addition, elements of Iran's Revolutionary Guard Corps (IRGC) have openly sought to pull hackers into the fold.[33] There is evidence that at the heart of IRGC cyber efforts one will find the Iranian political/criminal hacker group Ashiyane;[34] and the Basij, who are paid to do cyber work on behalf of the regime, provide much of the manpower for Iran's cyber operations.[35] In the event of a conflict in the Persian Gulf, Iran could combine electronic and computer network attack methods to degrade US and allied radar systems, complicating both offensive and defensive operations of the US and its allies.[36] In Hizbollah's own bid to deter, moreover, Hizbollah leader Hassan Nasrallah has stated publicly that there will be no distinction drawn between Israel and the United States in terms of retaliation, should Israel attack Iran to halt its progress toward a nuclear weapons capacity: "If Israel targets Iran, America bears responsibility."[37]

In sum, states are exploiting cyberspace to advantage, furthering their own interests by gathering information, gaining the ability to degrade the capabilities of perceived adversaries, and so on. Non-state actors, terrorists, and criminals are also leveraging cyberspace to their own ends, benefiting from a domain that levels the playing field and allows smaller and even

individual actors to have a disproportionate impact. This asymmetry gives rise to an ecosystem that is fraught with a range of perils that did not previously occupy the focus and energies of major powers. Hence the concerns of the major powers, for the impact of certain scenarios raised above could significantly undermine, if not shatter, trust and confidence in the system (be it American or another).

Nor is the threat unique to the United States. Asymmetric warfare is of course one of the defining features of the Israeli experience on both the kinetic and virtual battlefields.[38] Consider also other (arguably) lesser known casualties of the cyber struggle. As outlined by the Office of the National Counterintelligence Executive in its 2011 Report to Congress:

> Germany's Federal Office for the Protection of the Constitution (BfV) estimates that German companies lose $28 billion-$71 billion and 30,000-70,000 jobs per year from foreign economic espionage. Approximately 70 percent of all cases involve insiders.
>
> South Korea says that the costs from foreign economic espionage in 2008 were $82 billion, up from $26 billion in 2004. The South Koreans report that 60 percent of victims are small- and medium-sized businesses and that half of all economic espionage comes from China.
>
> Japan's Ministry of Economy, Trade, and Industry conducted a survey of 625 manufacturing firms in late 2007 and found that more than 35 percent of those responding reported some form of technology loss. More than 60 percent of those leaks involved China.[39]

Observations by French Senator Jean-Marie Bockel, recorded in an "information report" of France's Senate Committee on Foreign Affairs, Defence and Armed Forces, are equally striking:

> In France, administrative authorities, companies and vital service operators (energy, transport, health, etc.) are victims daily of several million cyber attacks....These cyber attacks may be carried out by computer hackers, activist groups, criminal organisations, as well as by competitor companies, or even by other States. The finger of suspicion often points towards China or Russia, even if it is very difficult to identify the authors of these attacks precisely.[40]

So too the assessment of Jonathan Evans, Director General of the United Kingdom's Security Service:

> Britain's National Security Strategy makes it clear that cyber security ranks alongside terrorism as one of the four key security challenges facing the UK. Vulnerabilities in the internet are being exploited aggressively not just by criminals but also by states. And the extent of what is going on is astonishing – with industrial-scale processes involving many thousands of people lying behind both State sponsored cyber espionage and organised cyber crime....One major London listed company with which we have worked estimates that it incurred revenue losses of some £800m as a result of hostile state cyber attack – not just through intellectual property loss but also from commercial disadvantage in contractual negotiations. They will not be the only corporate victim of these problems.[41]

Evans has reasoned further as follows:

> So far, established terrorist groups have not posed a significant threat in this medium, but they are aware of the potential to use cyber vulnerabilities to attack critical infrastructure and I would expect them to gain more capability to do so in future.[42]

The necessary question is, therefore, what should be done.

Cyber Deterrence and Multidimensional Response

Given the manifold and disturbing evidence of cyber capability and hostile intent on the part of both state and non-state actors, the United States must carefully chart and craft a way forward that comes to terms powerfully and proportionately with the facts and realities of concern that characterize the cyber domain today (and are unlikely to disappear any time soon). It would be false comfort to think that the US or its allies can firewall a way out of this problem. Instead, and in order to help shore up both cyber security and the protection of critical infrastructure, the US should formulate, articulate, and implement a cyber deterrence strategy.

A spirited but embryonic policy debate on the subject has already been held in certain select quarters, yet the complex, cross-sector, and multidisciplinary nature of the challenge has so far rendered a strategic, integrated response out of reach. Threats are evolving daily, adding an

extra layer of complication, and notwithstanding the pace and volume of the threat stream, information about threat vectors is often not shared across sectors or made public. At the level of principle, this reticence is certainly not beyond reason, as government seeks to protect classified material and industry seeks to protect proprietary information. In practice, though, such reluctance throws sand in the gears of response as well as prevention efforts.

Against this background the scale of the task is admittedly daunting, but the United States would be well served to elaborate and execute a cyber deterrence strategy and policy that seeks to dissuade, deter, and compel, both as a general matter and in a tailored manner that is actor/adversary-specific. A solid general posture meaning basic security steps (protection, hygiene, technology), could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This would free up resources (human, capital, technological) to focus in context-specific fashion on the remainder, which constitute the toughest threats and problems, in terms of their level of sophistication and determination. To make such recommendations operational, lines in the sand or, in this case the silicon, must be drawn. Preserving flexibility of US response by maintaining some measure of ambiguity is useful, so long as parameters are made clear by laying down certain markers or selected red lines whose breach will not be tolerated.[43]

To effectively deter an individual or entity and thereby prevent it from accomplishing its goal – or ideally, prevent it from acting in the first place – it is imperative to understand fully just what the initiating party hopes to achieve. (The idea is a variation on the theme/principle of noted strategist Miyamoto Musashi: "Know your enemy, know his sword."[44]) This foundational understanding constitutes the first step to dissuade or compel one's adversary; and taking that step requires examining the situation through the eyes of the other. While bearing in mind that all of the sources of threat referenced above are exploring and exploiting information and systems via cyber means, these various actors have different and distinct objectives. Though using virtual means in a virtual medium, each such actor is after specific real world results and seeks to collect (or worse) from its target(s) accordingly.

What must the United States do to convince state actors not to engage in computer network exploitation or computer network attack through their

military and intelligence services in furtherance of broader goals? Here the US cyber response should be an outgrowth of its broader deterrence strategy relative to a given actor, meaning that the cyber deterrence component should be consistent with and complementary to any preexisting, broader US deterrence strategy for that player. Other countries need to understand and appreciate that the United States can and will impose a proportionate penalty if attacked in a cyber manner and medium, though US response may ultimately be cyber or kinetic, with all options on the table. Regarding cyber response, offensive capability must be demonstrated in such a way as to leave no doubt as to the consequences of breaching a US red line. Such demonstration, however, must be undertaken with full recognition of the fact that any tool, technique, tactic, or procedure employed could subsequently be taken up, tweaked, and used in turn in retaliation, including against allies. Response in this context is predicated on the ability to attribute an attack to one or more specific actors (foreign powers).

On the intelligence side, since their inception states have been engaged in stealing secrets. Though espionage has gone digital, taking and adapting the world's second oldest profession to the twenty-first century, foreign governments are using cyber means for the original purpose: to obtain information that can be used to shape and sharpen decision making. Put another way, states are using cyber means (think of Russian and Chinese hackers working in service of their governments, for example) to augment their ability to collect information of interest to their respective policymakers. The question then becomes, what information are these actors interested in obtaining, and why? To the extent that practitioners of cyber deterrence can inject insights and articulate a detailed answer to this double-barreled query, the targeted government (be it US or allied) will be able to defend systems better and tailor deterrence activities correspondingly.

Industrial espionage is a subset of this type of state sponsored activity. The intent is to increase the economic prosperity or viability of business concerns in a given state. Although the espionage activity is state directed, the ultimate beneficiaries may be private or semi-private entities. On the flip side, from the target's perspective, the consequences that follow from the theft of trade secrets may be profound and extend beyond economic loss, to diminished national stature in the eyes of the world. In the assessment of US National Counterintelligence executive Robert "Bear" Bryant, cyber-

espionage is "a quiet menace to our economy with notably big results.... Trade secrets developed over thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors."[45] US productivity and innovation may also suffer as a result, with further potential knock-on effects for future growth and development. If military relevant information is exposed and extracted, there may also be national security implications. It takes little imagination to conjure up what a hostile party could do, for example, with stolen US technology that holds potential military application.[46]

Much like states, transnational terrorist organizations seek an asymmetric advantage that they can leverage in trying to enact their desired political agenda. By and large, however, such groups possess fewer resources than states, and have largely eschewed engaging in the political process, favoring instead the use of violence to achieve their aims. From this standpoint it would not be much of a stretch for terrorists to seek more bang for their buck, by turning to digital means as a force multiplier for kinetic action. The more detail that can be learned and discerned about these groups' tactical cyber and strategic political objectives and aspirations, the more helpful fodder there will be for crafting a cyber deterrent that thwarts them.

The forces of terror and crime may also converge, merging into a hybrid threat founded on an alliance of convenience, in which each party draws on the other's skills and assets to further their respective ends. Contrary to their non-state counterparts whose mainstay is crime alone, pure and simple profit is not what makes terrorist groups tick. This difference in kind actually presents an opening of sorts, which could be exploited through skillful exposition and execution of a tailored cyber deterrence strategy.

Recall that deterrence is a subset of coercion that seeks to cause an adversary to refrain from acting by influencing its belief that the likelihood of success is slight, or that the pain from the response is greater than it is willing to bear.[47] Historically, deterrence has been taken to require "three overt elements: attribution, signaling, and credibility."[48] In present context, deterrence presupposes that the contours of US red lines are made clear to its adversaries as well as its allies; that it has signaled that breaches of these boundaries will not be tolerated; and that it can and will visit consequences for any such breach upon the party that trespasses. The

expected US reaction should be sufficiently threatening to the potential perpetrator to dissuade it from undertaking the activity in the first place.

When defining US red lines in cyberspace, substantial forethought and caution must be exercised, bearing in mind that activities that approach but do not cross these lines will, as a corollary of boundary definition, be considered from a less punitive perspective. Activities that do not have an otherwise benign purpose, such as efforts to map US critical infrastructure, should be assessed accordingly. Nothing good can come when a foreign country or non-state actor has intimate knowledge of these systems.

Attribution is crucial to underpin deterrence. One must know who has acted in order to visit consequences upon them. However, it is hard to find a smoking keyboard in cyberspace since the domain is made for plausible deniability. The magnitude and significance of the attribution challenge in the context of cyber attack response has been underscored by prominent analysts,[49] though a contrarian strain does exist.[50] Difficulty aside, being able to attach the action to the actor enables the aggrieved party to react. The possibility of response in kind increases the number of options that a targeted entity can draw upon after the fact, which could include the potential to give better than the original target may have gotten. Concerted effort directed towards developing improved attribution capacities through technological and other means are time and resources well spent.

So too must adversaries understand and appreciate that the United States stands poised to use the full spectrum, breadth and depth, of its powers to enforce these rules. To credibly convey that message and have it hit home with those who bear hostile intent, there must be a public display of capabilities that is sufficient to make the point, without exposing so much that the display becomes self-defeating because it gives away the store, by permitting adversaries, for example, to reverse engineer (or otherwise mimic) and use the very US means and methods that are on display. The "display" aspect of the exercise is made even trickier by the fact that the laws governing cyber warfare are still nascent, evolving, and thus to some extent unclear. Caution and proceeding with care are therefore warranted on a second level as well.

Although the United States must demonstrate that it has in its toolkit the requisite items for use against hostile parties when necessary, there has not been a clear cut public demonstration of cyber dominance to date for which the US has definitively taken and actively sought ownership.

Against this background, should the United States consider engaging in the digital equivalent of an above-ground nuclear test? This is a question for US policymakers, practitioners, and technologists alike, as they seek to define a path forward and elaborate both doctrine and strategy for the cyber domain. The ironic possibility that if conducted with care (commensurate to the enormity of the exercise) the cyber equivalent of such a test may be instrumental to deterring hostile actors and thereby preclude a fight is not to be dismissed out of hand.

Building Stability through Strength

It is sometimes said that the best defense is a good offense. According to open source reports, the United States is developing rules of engagement regarding cyber attacks, and the Defense Department is seeking to bolster its arsenal of cyber weapons[51] (though a cyber attack may engender a cyber or kinetic response). As former Vice Chairman of the Joint Chiefs of Staff General James E. Cartwright has observed, efforts and investments of the type just described would help recalibrate the defense to offense ratio – which until relatively recently stood at 90 percent to 10 percent in favor of defense[52] – and would strengthen and build credence in the US ability to deter effectively adverse action in the cyber domain.

However, the US cyber security community, like its allied counterparts, remains a work in progress. In the US in particular, the community still has a long way to go before it reaches the level of skill and maturity now displayed by the US counterterrorism community.[53] The synchronization of Titles 10 and 50 of the United States Code, harmonizing military and intelligence functions, has been a major post-9/11 breakthrough that significantly enhanced the US overall counterterrorism posture. The US can leverage this achievement by tailoring and applying the concept to the cyber context, bearing in mind the (yet-to-be-met) twin challenges of codifying rules of engagement and pursuing a more proactive stance.[54]

To move forward smartly in the cyber domain, the United States and its allies must demonstrate leadership and possess vision, together with a sound plan of action. For too long, incidents have driven strategy – in effect, tactics masquerading as strategy. While the United States possesses some unique capabilities, these capabilities will not be used to fullest advantage unless and until there is a broader strategic framework in which to embed them. Building on the conceptual framework set out above, certain key

tenets emerge that can serve as a foundation for developing and enacting an effective cyber deterrence strategy, capacity, and posture. Those tenets, the beginnings of a blueprint for cyber deterrence, are as follows:

Calibrate to meet the mission. Capability supports credibility in this context. To the extent that investments and efforts may reflect a defense to offense ratio that suggests an imbalance that could negatively impact on homeland/national security, the existing calibration should be considered carefully and adjusted as necessary. As a prerequisite to imposing consequences, calibration (or recalibration) goes hand in hand with the political will to act, when called upon, to impose sanctions.

Start and build from a position of strength. To deter or dissuade successfully requires the capacity to convince potential adversaries that the costs of hostile action will exceed the perceived benefits. Developing and signaling the existence of a first strike capability is therefore fundamental.

Put the accent on speed, surprise, and maneuverability. Nanoseconds can make a difference in cyberspace. Response in close to real time should therefore be the goal. While there should be no doubt about the principle that any breach of red lines will incur consequences, there is value in maintaining a measure of ambiguity about the precise nature of those consequences, so as to keep the object looking constantly over its shoulder. Flexibility plus clarity may seem a non sequitur, but in fact is strategically prudent here.

Leave no person behind. A first strike capability alone would leave the country vulnerable to and unprepared for a response in kind, should the adversary possess such capacity. As in the Cold War stage of the nuclear era, both prudence and forethought mandate a second strike capability to ensure force protection. Maintaining dominance in science and technology is crucial, since there are technical solutions to even vexing challenges in the cyber domain.

Know thy adversary. The maxim may be worn and tired, but it still applies. To defeat potential adversaries, a deep understanding of the particular aims and aspirations of each is needed. This insight should then inform the strategy and tactics for that case, allowing these elements to be tailored to a specific opponent, thereby maximizing the potential to thwart them. The so-called "OODA loop" – observe, orient, decide, and act – applies.

Lead by example. Implicit in the idea of robust cyber deterrence is the presupposition that the entity poised to deter has inoculated itself against that which it may visit upon others (since the possibility of blowback exists). To proceed differently is to jump off the plane without a parachute. The US government should therefore strive to place its own house in order as a crucial corollary to meeting the threat. Moreover, the government should initiate the steps needed to facilitate information sharing so that critical facts reach all key defenders of national assets and resources, including those owned and operated by the private sector (critical infrastructure).

Partner for success. No single component of government or even the government as a whole can go it alone in the cyber domain. Genuine intra- and cross-sector partnerships are essential. Within government, for example, the careful synchronization and harmonization of military and intelligence functions (Titles 10 and 50) for cyber deterrence purposes could prove valuable, as it has in the counterterrorism context. The importance of inoculating ahead of time extends beyond the public sector to critical networks and systems that lie in private hands. Accordingly, the private sector must commit to undertake the steps necessary to reinforce homeland/national security. To ensure that bar is met, federal authorities should reach out to the private sector, taking a carrot and stick approach that combines both positive and negative incentives designed to produce the desired outcome.

Think and act internationally. Transnational challenges require transnational solutions, and cyberspace is by definition borderless. Trusted partners on the international level can and should bring much to the table in this context. Admittedly, national interests may impede the ability to share the most sensitive of data and information. Nevertheless, it would be self-defeating to refrain from leveraging key bilateral relationships and alliances, from the "Five Eyes" intelligence partnership (Australia, Canada, New Zealand, the United States, and the United Kingdom) to NATO to the EU plus other strategic partners such as in the Mediterranean region and Asia, to include Israel, Singapore, India, and Japan.

With inspired leadership – the cyber warfare equivalents of Billy Mitchell, Bill Donovan, or George Patton, who truly understood the tactical and strategic uses of new technologies and weapons – the United States can forge and execute a powerful cyber deterrence strategy that looks through

its adversaries' eyes in order to be adequately prepared for cyber events, ideally with just bits and bytes rather than bullets, bombs, and bloodshed.

Notes

1 Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe," in *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century* (Washington, D.C.: George C. Marshall Institute, 2011), p. 27.

2 Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation, March 7, 2012, p. 54, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

3 Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html; and Mark Clayton, "Exclusive: Potential China Link to Cyberattacks on Gas Pipeline Companies," *Christian Science Monitor*, May 10, 2012, http://www.csmonitor.com/USA/2012/0510/Exclusive-potential-China-link-to-cyberattacks-on-gas-pipeline-companies.

4 Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* (October 2011), p. 4, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

5 Ibid.

6 Eben Kaplan, *Terrorists and the Internet*, Council on Foreign Relations, January 8, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005; and Special Report by the Homeland Security Policy Institute (HSPI) and the University of Virginia's Critical Incident Analysis Group (CIAG), *NETworked Radicalization: A Counter-Strategy* (Washington, D.C.: May 2007).

7 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

8 See Thomas C. Schelling's classic text, *Arms and Influence* (New Haven: Yale University Press, 1966).

9 See for example Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation,2009).

10 Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (New York: Oxford University Press, 1963).

11 Ellen Messmer, "DHS: America's Water and Power Utilities under Daily Cyber-Attack," *Network World*, April 4, 2012, http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?t51hb&hpg1=mp.

12 Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily," *US News & World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

13 Joe Lieberman, "Cyber Networks Sitting Ducks for Attacks" *Hartford Courant*, April 8, 2012, http://articles.courant.com/2012-04-08/news/hc-op-lieberman-cyber-security-biggest-national-th-20120408_1_cyber-attack-cyber-networks-cyber-threats.

14 John O. Brennan, "Time to Protect against Dangers of Cyberattack," *Washington Post*, April 15, 2012, http://www.washingtonpost.com/opinions/time-to-protect-against- dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.

15 Lieberman, "Cyber Networks Sitting Ducks for Attacks."

16 Jason Ryan, "FBI Director Says Cyberthreat will Surpass Threat from Terrorists," January 31, 2012, http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

17 "'The reality is that our infrastructure is being colonized,' said Tom Kellerman, former commissioner of President Obama's cyber security council." See David Goldman, "Cybersecurity Bills Aim to Prevent 'Digital Pearl Harbor,'" April 23, 2012, http://money.cnn.com/2012/04/23/technology/cybersecurity-bills/?source=cnn_bin.

18 "A senior intelligence official, briefing reporters on the condition of anonymity, noted a few cases in which estimates were given in economic espionage prosecutions over the past six years: $100 million worth of insecticide research from Dow Chemical, $400 million worth of chemical formulas from DuPont, $600 million of proprietary data from Motorola, $20 million worth of paint formulas from Valspar." See Ellen Nakashima, "In a World of Cybertheft, U.S. Names China, Russia as Main Culprits," *Washington Post*, November 3, 2011, http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html.

19 Nick Hopkins, "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article; and Nick Hopkins, "US and China Engage in Cyber War Games," *The Guardian*, April 16, 2012, http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=article.

20 Reuters, "Saudi Oil Producer's Computers Restored after Virus Attack" *New York Times*, August 26, 2012, http://www.nytimes.com/2012/08/27/technology/saudi-oil-producers-computers-restored-after-cyber-attack.html?_r=1.

21 Elinor Mills, "Virus Knocks out Computers at Qatari Gas Firm RasGas," *CNET News*, August 30, 2012, http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/.

22 Christopher Brook, "Report: French Nuclear Company Areva Hit by Virus," *ThreatPost*, October 31, 2011, http://threatpost.com/en_us/blogs/report-french-nuclear-company-areva-hit-virus-103111.

23 Michael McCaul, Chairman of the House of Representatives Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management, said: "China is the most aggressive collector of U.S. economic information and technology...China's cyber warfare capabilities and the espionage campaigns they have undertaken are the most prevalent of any nation state actor. China has created citizen hacker groups, engaged in cyber espionage, established cyber war military units." See NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 5; see also Cindy Saine, "Experts Warn of Increased US Cyber Security Threat," *VOA News*, April 24, 2012, http://www.voanews.com/english/news/usa/Experts-Warn-of-Increased-US-Cyber-Security-Threat-148786975.html.

24 Qiao Liang and Wang Xiangsui, published by China's People's Liberation Army, Beijing.

25 David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf.

26 Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" *Atlantic Council Issue Brief* (2011), p. 2, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf.

27 Group IB, *State and Trends of the Russian Digital Crime Market 2011*, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf; see also http://group-ib.com/images/media/Group-IB_Cybercrime_Inforgraph_ENG.jpg (graphics).

28 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," Testimony before the House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, April 26, 2012, p. 4, http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf; and Conficker Working Group, *Conficker Working Group: Lessons Learned*, http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

29 Cilluffo, Testimony before the House of Representatives, p. 4.

30 Jack Clohurty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad,'" *ABC News*, May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UEieyEQrOlg.

31 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

32 Cilluffo, Testimony before the House of Representatives, p. 6.

33 Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," Radio Free Europe, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html.

34 Iftach Ian Amit, "Cyber [Crime/War]," paper presented at DEFCON 18 conference, July 31, 2010.

35 "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah*, March 24, 2011, http://internet-haganah.com/harchives/007223.html.

36 Michael Puttre, "Iran Bolsters Naval, EW Power," *Journal of Electronic Defense* 25, no. 4 (2002), p. 24; Robert Karniol, "Ukraine Sells Kolchuga to Iran," *Jane's Defense Weekly* 43, no. 39 (September 27, 2006), p. 6; Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

37 Reuters, "Nasrallah: Iran could Strike US Bases if Attacked," *Jerusalem Post*, September 3, 2012, http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706.

38 Ilan Evyatar, "Falling into the Trap, Over and Over Again," *Jerusalem Post*, November 17, 2010, http://www.jpost.com/Features/InThespotlight/Article.aspx?id=195767; Dan Harel, "Asymmetrical Warfare in the Gaza Strip: A Test Case," *Military and Strategic Affairs* 4, no. 1 (2012): 17-24, http://www.inss.org.il/upload/(FILE)1339053338.pdf; Yolande Knell, "New Cyber Attack Hits Israeli Stock Exchange and Airline," *BBC News*, January 16, 2012, http://www.bbc.co.uk/news/world-16577184; and Joshua Mitnick, "Israel's Businesses Losing the Cyber War," *Wall Street Journal*, July 25, 2012, http://online.wsj.com/article/SB10000872396390443477104577549262451192148.html.

39 NCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, p. 19.

40 Jean-Marie Bockel, Senator for Haut-Rhin, "Cyber Defence an International Issue, a National Priority," *Information report no. 681 – Committee on Foreign Affairs, Defence and Armed* Forces, July 18, 2012, www.senat.fr/rap/r11-681/r11-681-syn-en.pdf.

41 Address at the Lord Mayor's Annual Defence and Security Lecture, City of London, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html.

42 See Tom Whitehead, "Cyber Crime a Global Threat, MI5 Head Warns," *The Telegraph*, June 26, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html.

43 Cilluffo, Testimony before the House of Representatives, pp. 7-8. See also Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats," *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012), http://www.afpc.org/files/august2012.pdf; and Martin C. Libicki, "The Strategic Uses of

Ambiguity in Cyberspace" *Military and Strategic Affairs* 3, no. 3 (2011): 3-10, http://www.inss.org.il/upload/(FILE)1333532281.pdf.

44 *The Book of Five Rings.*

45 Nakashima, "In a World of Cybertheft, U.S. Names China, Russia as Main Culprits."

46 Ibid.

47 W. W. Kaufmann, "The Requirements of Deterrence, " in W. W. Kaufman, ed., *Military Policy and National Security* (Princeton: Princeton University Press, 1956); Peter Marquez, "Space Deterrence: The Pret-a-Porter Suit for the Naked Emperor," in *Returning to Fundamentals*, pp. 9-10. Coercion in turn seeks to influence an adversary to act or refrain from acting by threatening to, or actually, imposing costs on an adversary to limit its options and/or affect its cost/benefit analysis such that the adversary determines the cost of its putative action is not worth the benefit that would be conferred. Marquez, "Space Deterrence," p. 10, citing G. Schaub, Jr., "Deterrence, Compellence and Prospect Theory," *Political Psychology* 25, no. 3 (2004): 389-411.

48 Marquez, "Space Deterrence," p. 10.

49 For example, see Yasmin Tadjdeh, "U.S. Military Overestimates Value of Offensive Weapons Cyberweapons, Expert Says," *National Defense*, September 13, 2012, citing Martin Libicki, senior management scientist at RAND Corp, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=887.

50 F. Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." Paper presented at the Cyber Conflict (CYCON), 2012 4th International Conference, June 5-8, 2012.

51 Federal News Radio, "DoD Hammering out Rules of Cyberspace," October 21, 2011, http://www.federalnewsradio.com/?nid=398&sid=2602063; and Ellen Nakashima, "Pentagon to Fast-track Cyber Weapons Acquisition," *Washington Post*, April 9, 2012, http://www.washingtonpost.com/world/national-security/pentagon-to-fast-track-cyberweapons-acquisition/2012/04/09/gIQAuwb76S_print.html.

52 Lolita C. Baldor, "Pentagon to Publish Strategy for Cyberspace War," *Navy Times,* July 14, 2011, http://www.navytimes.com/news/2011/07/ap-pentagon-publish-strategy-cyberspace-war-071411/; see also "A Conversation on Cyber Strategy with General James E. Cartwright," *Homeland Security Policy Institute (HSPI) Capstone Series on Cyber Strategy*, May 14, 2012, http://www.gwumc.edu/hspi/events/cartwrightCS501.cfm.

53 Frank Cilluffo and Andrew Robinson, "Analysis: While Congress Dithers, Cyber Threats Grow Greater," *Nextgov*, July 24, 2012, http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/.

54 Cilluffo, *AFPC Defense Dossier*.