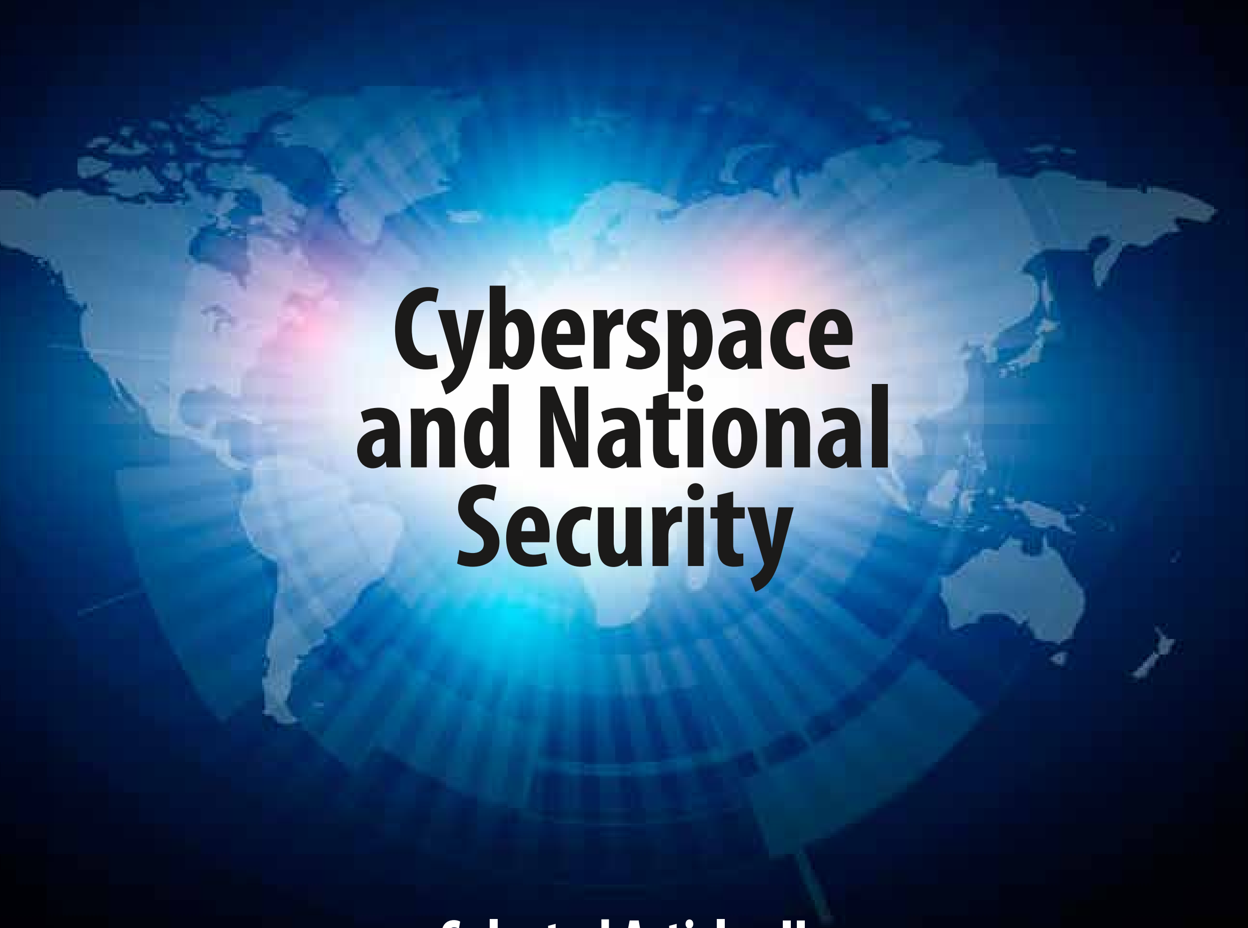

Cyberspace and National Security

Selected Articles II

Edited by Gabi Siboni

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE
CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Cyberspace and National Security

Selected Articles II

Edited by Gabi Siboni

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE
CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Graphic design: Michal Semo-Kovetz
Printing: Elinir

Institute for National Security Studies
(a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556

Tel. +972-3-640-0400
Fax. +972-3-744-7590

E-mail: info@inss.org.il
http://www.inss.org.il

March 2014

ISBN: 978-965-7425-59-6

INSS Institute for National Security Studies

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006.

The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda.

INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public.

INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the author's alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organization and individuals that support its research.

Contents

Foreword

Israel's rapid development as a leading player in the cyber realm is one of several factors that have spurred research in Israel in general, and at the Institute for National Security Studies (INSS) in particular, on cyber-related issues. In order to broaden the scope of the research underway at INSS, the INSS Cyber Program has long promoted international cooperation in the field, reflected, for example, in the INSS conference on defensive operations and intelligence in cyberspace, held with the Cyber Security Forum Initiative (CSFI), a large and important organization in the United States cyber community. This year's conference is also held in collaboration with various entities in Israel, including the Ministry of Intelligence, the National Cyber Staff, the IDF Computer Service Directorate, and the chief scientist in the Ministry of the Economy.

The conference's focus on defensive operations and intelligence allows INSS to highlight its work in this field, which complements a variety of related professional activities underway in Israel and around the world. This year's conference has several important objectives, among them: to deepen cooperation among government agencies and organizations in the cyber field in Israel and the United States; to enhance exposure of the Israeli cyber market among American technology companies that seek to develop business in Israel or to lend exposure to Israeli capabilities and technologies abroad; and to expand international cooperation in the cyber field with other countries.

As with previous conferences, we have compiled several articles written by researchers at INSS and institutions elsewhere around the world. These articles were prepared within the framework of the Institute's Cyber Program, and were first published in the INSS journal *Military and Strategic Affairs*.

Gabi Siboni
Director, Cyber Program, INSS

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.

In order to help structure the debate and advance toward the goal, we propose a framework that examines the issue critically and looks to

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.

This article was first published in *Military and Strategic Affairs* 4, no. 3 (2012): 3-23.

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*.

Duqu’s Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyberwar

Matthew Crosston

The debate over the applicability or non-applicability of international law to cyberwar and the need for a cyber-specific international treaty might be irrelevant. Both camps, pro and con, argue about the need for cyberwar to have the Law of Armed Conflict (LOAC) or some new international legislation properly cover the cyber domain. Both camps, however, misread how the structure of the cyber domain precludes strategically “piggybacking” on conventional norms of war. International laws on conventional war are effective because of the ability to differentiate between civilian and military sectors. There is a civilian/military ambiguity in the cyber domain that makes such differentiation unlikely if not impossible well into the future.

Hence “Duqu‘s Dilemma”: with the focus on establishing legitimate targets and setting limitations on allowable action, the United States and its allies expose themselves to vulnerabilities while engaging in a futile endeavor that does not lead to improved cyber control. The effort to establish cyber rules akin to conventional norms is fruitless since these rules are not enforceable or logical. They will simply handcuff lawful states. This signifies that greater effort should be expended on creating preemptive strategy that accepts the military/civilian ambiguity problem. The tendency of scholars and policymakers to strive for “sanitized” cyberwar by constraining targets during operations means that cyber strategy remains devoid of true deterring power.

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and Founder and Director of the International Security and Intelligence Studies (ISIS) program at Bellevue University.

This article was first published in *Military and Strategic Affairs* 5, no. 1 (2013): 119-31.

Whether one believes LOAC can or cannot apply to the cyber domain, whether one pushes for an international cyber treaty or thinks such treaties will be meaningless, one aspect is constant: the desire for rules governing cyberwar behavior. The problem is in attempting to create a code of cyber conduct that demands a distinct separation between civilian and military sectors. The cyber domain is not amenable to this separation since the aforementioned fusion, where participants, facilities, and targets are hopelessly entangled between civilian and military institutions, has basically been a missing explanation as to why the global effort to enhance and clarify norms has remained uneven and inadequate.

The Ineffectiveness of International Law

Addressing the issue of cyber security, the East-West Institute stated in 2011, "There is an urgent need for international cooperation on this most strategic of issues. If we fail on this task, global stability could be as threatened as it would be by a nuclear exchange."[1] International norms established with the Geneva and Hague conventions were meant to be explicit lines of protection for civilian populations when states engaged in war. That respect for and preservation of civilian life is now held to be sacrosanct, regardless of what form or delivery method war takes. As such, there is an expectation that cyberspace can be subjected to the discipline of conventional norms.

Others argue that establishing these customary understandings in the cyber domain is one of the most important geopolitical battles today, going so far as to say that it is Ground Zero for global diplomacy, national security work, and intelligence.[2] The goal is to bring the principles of arms control into the cyber domain. Indeed, the most optimistic want voluntary agreements that impose constraints on the development of cyber capabilities and ostensibly ameliorate behavior in cyberspace. Some, however, have acknowledged that there are potential dangers in trying to achieve this. Stewart Baker, a former general counsel at the NSA and assistant secretary for policy at DHS under President George W. Bush, voiced the obvious fear: the United States and its allies would obey whatever was written down and agreed to while no adversaries would.[3]

There may be a larger problem, however, than non-compliance: conventional war has the distinct advantage, historically, of being fairly explicit about target classification. Most military networks that would initiate and enact a cyber attack depend upon and work within countless numbers of civilian networks. In addition, many of the actors that are part of the planning, initiation, and deployment of cyber attacks are not necessarily formal military but rather civilian employees of government agencies. In other words, the world of cyber conflict and cyberwar is not a world that can achieve such explicit classification. In fact, future trends only show this fusion growing deeper and tighter in time. As such, any attempt to introduce norms and rules that are predicated upon knowledgeable differentiation will likely end up confused and ineffective.

This "ambiguity assertion," for lack of a better term, has so far been relatively ignored in the various cyber debates. The latter tend to revolve around how loose or rigid, how informal or formal, how international or local such codes of constraint should be. Many of these proposed codes aim to constrain cyber behavior so as to protect banking, power, and other critical infrastructure networks "except when nations are engaged in war."[4] Without addressing the ambiguity problem, however, states find themselves in a quandary: where are the lines of distinction between civilian and military drawn? Perhaps the biggest dilemma, therefore, is not the problem of figuring out attribution (who was the trigger man), but rather this futile attempt to clear up the inherent and purposeful ambiguity that characterizes the critical infrastructure used to house, develop, and utilize a state's cyber capabilities.

Many of the current cyber discussions are flawed by the manner in which they implicitly want to analogize conventional conflict with cyber conflict, to make cyber attacks equivalent to armed attacks. To do this, however, the conversation must turn to legal definitions and parameters: when does cyber conflict constitute the use of armed force or a formal act of war? What actions would constitute a war crime? How much damage does it take to trigger a necessary retaliatory response?[5] These questions are much more difficult to answer in the cyber realm because of the logistical nightmare provoked by the ambiguity assertion. This fact has not been emphasized appropriately to date, nor is it strategically addressed at all.

Up to now, questions have focused instead more on comparable lethality, damage estimates, and the aforementioned attribution problem. To an extent, however, all of these problems are enveloped by the civilian/military ambiguity issue. The inability to establish that separation means that lethality could be more extreme by being more than just military casualties, damage could be more devastating by being more than just military facilities, and attribution might not even be relevant: defining the WHO of an attack does not solve the problem if the HOW behind the WHO is inextricably fused among government, military, and civilian properties and people. In other words, many assume that figuring out WHO in cyberwar will solve most problems. The ambiguity assertion reminds everyone to be careful what they wish for: in cyber war, the WHO will never be conveniently distinct because of the HOW.

International law clearly does not alleviate the problem of civilian/military ambiguity in cyber conflict. Whether the discussion extends to codes of conduct, treaties, or international laws writ large, none of these potential documents attempts to address the inherent structural problem of modern societies and how they currently organize, conduct, and develop their cyber capabilities. Further confirming this is the equal amount of time, effort, and frustration expended in the sister projects of establishing terms and defining parameters. Examining that frustration will illustrate how impactful the ambiguity assertion is when contemplating how the world should deal with the rules for cyberwar.

The Frustration of Setting Terms

Part of the problem in getting international law to cover cyberspace efficiently involves a longstanding failure to translate essential terms and parameters into something that would truly impact on the cyber domain. Progress in moving beyond this problem has been extremely limited. Indeed, even a cursory glance across the literature over the past decade attests to the fact that cyberwar does not fit perfectly into the already existing legal frameworks on war and use of force.[6] Despite this reality, these terminological and doctrinal difficulties have been continually investigated with the aim of forcefully coordinating existing terms and doctrines in the cyber arena. This article argues that the lack of success is attributable to the unwillingness to engage the civilian/military fusion.

The desire for explicit terms, parameters, definitions, laws, and treaties is based more on the worry that failure to produce such explicitness will leave cyberwar outside the boundaries of rules that currently govern conventional war. The consequences are considered stark: critical civilian infrastructure could be targeted, as could basic necessities such as agriculture, food, water, public health, emergency services, telecommunications, energy, banking and finance, and so on. The ambiguity assertion, however, articulates the difficulty in obtaining such explicitness: most if not all of a state‘s cyber capability utilizes and depends upon critical civilian infrastructure that also provides many important civilian functions. No state to date has created a cyber operations capability that is wholly distinct and separate from civilian networks and civilian infrastructure. In other words, go after the "military" targets and you will also de facto be going after "civilian" targets. The literature to date seems to ignore this fact. Consequently, much of the literature engages in a false riddle, trying to impose a theoretically precise answer on an empirically ambiguous reality.

This is further confirmed by the number of respected scholars, diplomats, and policymakers who miss the relevance of the ambiguity assertion by demanding that the laws of cyberwar should actually *forbid* the targeting of purely civilian infrastructure, indicating that cyber actors should try to respect the Geneva Conventions as much as conventional actors do.[7] The problem, of course, is that in cyberwar, purely civilian infrastructure is a category of diminishing returns. Indeed, given the obvious trend that sees only intensification and deepening of the civilian/military fusion, purely civilian infrastructure will end up more myth than reality.

The failure to address this structural riddle has been matched by an over-emphasis on agency. This manifests itself mainly in the focus on limiting and controlling potential cyber actions from adversarial states. James Lewis of CSIS emphasizes how a state can reduce risks for everyone by imposing common standards, like moving from the Wild West to the rule of law.[8] Eugene Spafford concurred, citing how cyber security is a process, not a patch, requiring continual investment for the long term as well as the quick fix, without which states will always be applying solutions to problems too late.[9] These are some of the brightest and most respected names in the cyber discipline. Their warnings are not irrelevant, but the emphasis on state actor agency, while failing to recognize the impact and importance of inherent cyber structure, leaves a vulnerable gap in cyber strategic thinking. Indeed, the contemporary failure to create explicit norm coordination should be seen as a demand to consider new strategy that can accept this structural incompatibility as inherent and not something to "overcome." For structural ambiguity is not only intrinsic: states are purposely deepening the ambiguity for its strategic advantage and economic efficiency. States, therefore, should not focus on how to force a distinct civilian/military separation, but should rather develop new strategic thinking that accepts the ambiguity problem as a logistical reality that must be accounted for.

For empirical confirmation of the futility of trying to address these problems of conventional norms and explicit parameters, look no further than the United States military over the past half-dozen years. It is easy to produce a laundry list of frustration and unfulfilled hopes: General Alexander of US Cyber Command mentioned that progress was being made, but that the risks were nonetheless growing faster than the progress at present;[10] Vice Admiral Michael Rogers, commander of the US Navy's fleet cyber command, admitted to Congress that no agreement had been reached amongst the various commands on ironing out the rules of cyber conflict, but hoped that there would be positive developments "at some point in the near term";[11] and even the Pentagon produced a cyber document that ultimately stated that the laws of armed conflict apply in cyberspace as in traditional warfare, even while admitting that the basic terms "act of war" and "use of force" were still somewhat *ill-defined* in the cyber domain.[12] This shows the real term effects that the lack of new strategic thinking has when states do not address the ambiguity of civilian/military fusion.

Turf Wars and Tightropes: Military Discussion on Cyber Parameters

Just as with scholars, policymakers, and diplomats, the military has been steadfastly committed to establishing strict rules of cyber engagement that are akin to the conventional rules of war.[13] For several years, there has been a pending revision of the military's standing rules of engagement in the cyber realm.[14] It seems that while the military hoped that the scholarly and diplomatic communities would be able to help define much of the needed clarification, the two latter communities were themselves hoping to see the military lead the way with its revision. This obfuscation of responsibility, however, is not as relevant as many observers and analysts might think: failure to address these issues is not so much a case of one community trying to pass the buck on to another, but rather testimony to the confusion created when the ambiguity assertion about civilian/military fusion is not addressed.

General Alexander stated that in debating the rules of conflict in cyber operations, the United States was trying to do the job right.[15] Those debates, however, constantly oscillate back and forth between positions that do not address the primary innate structural concerns of the cyber domain. Consequently, the military has spent a half-dozen years promising imminent progress that does not materialize. The Pentagon's official report was itself described as ″ducking“ a series of important fundamental questions, including defining such basic terms as ″war,“ "force," and "appropriate response."[16] This is pointed out not to poke fun at the military. Quite to the contrary, this article makes the argument that given the reluctance of all parties concerned to engage the ambiguity assertion, with an eye to developing new strategy that embraces it rather than hopelessly using old strategy to overcome it, the military has had no real chance of making substantive progress to define the parameters of cyber action concisely.

It is no coincidence that the American military has sincerely worked on issues such as administrative network control, cyber organization, force composition, and cyber intelligence/operation differentiation, in addition to basic terminology parameters, without any major questions being considered definitively and comprehensively closed.[17] How, for example, can USCYBERCOM be expected to connect all the dots and be the competent arbiter in determining a case for action when it readily admits difficulty in even articulating who exactly comprises the fraternity of cyber warriors operating and defending home networks?[18] If the issues at hand were neither so serious nor so far-reaching on the future of cyber conflict, it would be almost comical. Only recently has it seemed possible that relevant military bodies have started to reach the epiphany discussed here:

> Although there are some noteworthy first steps toward establishing an international set of cyber norms – evident in bodies such as the Convention on Cybercrime – any global framework governing military response actions in cyberspace will surely materialize at an onerous pace. After all, how can the rules of war, built upon the tactile presence of combatants and weapons and sovereign territory, be retooled for a world where ′troops‘ can be dispatched in milliseconds from a multitude of states?[19]

At least the above quote begins to frame the discussion around the innate incompatibility between how war in cyberspace would likely be conducted and how that compares to all previous wars. It is still, however, emphasizing agency over structure: establishing an international set of cyber norms mainly to hallmark the division between civilian and military assets and mitigate action already undertaken. This might help explain why formal strategic documents concerning cyberspace end up being nothing but simple platitudes about how the United States intends to protect itself. Take for example the Department of Defense's (DoD) Strategy for Operating in Cyberspace, released in mid-2011 and consisting of five "strategic initiatives":

> *Strategic Initiative 1*: Treat cyberspace as an operational domain to organize, train, and equip so that the DoD can take full advantage of cyberspace's potential.
> *Strategic Initiative 2*: Employ new defense operating concepts to protect domestic networks and systems.
> *Strategic Initiative 3*: Partner with other US government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
> *Strategic Initiative 4*: Build robust relationships with US allies and international partners to strengthen collective cyber security.
> *Strategic Initiative 5*: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Take full advantage; employ new concepts; partner with others; build robust relationships; leverage ingenuity. All of these phrases are wonderful slogans, but they are not accompanied by any explicit new strategic thinking that could hope to actually institute said initiatives. Trying to adapt conventional strategy slightly and then force the cyber domain into it is likely to remain a project bearing little fruit. Examining that conventional strategy and proposing new strategy that engages the structural dilemma is the final section of this paper.

Engaging Ambiguity: Strategic Thinking for the Civilian/Military Cyber Fusion

The need for a new strategic approach is best illustrated when the arguments of two highly respected strategic thinkers – one military and one legal, who happen to fall on opposite sides of the LOAC cyber debate – ignore the problem of civilian/military structural cyber fusion. Dunlap, while accepting the need for improvement, believes the tenets of the law of armed conflict to be sufficient to address the most important issues of cyberwar.[20] The concern for distinguishing between legitimate military and civilian targets does not seem to bother Dunlap in its impact on the applicability of LOAC:

> LOAC tolerates ″incidental losses“ of civilians and civilian objects so long as they are ″not excessive in relation to the concrete and direct military advantage anticipated.“ In determining the incidental losses, cyber strategists are required to consider those that may be reasonably foreseeable to be directly caused by the attack. Assessing second- and third-order ″reverberating“ effects may be a wise policy consideration, but it does not appear LOAC currently requires such further analysis.[21]

Dunlap‘s distinction is actually quite important given the current intellectual climate: he has introduced some much-needed realism into the debates by reminding people that LOAC has never been a flawless strategy that provides perfect protection for civilians and civilian objects. The problem highlighted here, however, is that his concerns over military/civilian differentiation are misplaced.

These pro-LOAC arguments are effectively built around the fact that cyberwar does not have to have a perfect record in delineating and then protecting civilians because LOAC does not, either. But these arguments assume that such delineation is generally possible. The future of cyberwar is unlikely to be able to create such possibility because it has long been established how many of the military‘s critical functions, assets, service providers, and supply chains all rely heavily on civilian traffic and networks.[22] As such, new strategy needs to be positioned so as to prevent the use of cyber weapons in general, because once they are used, the likelihood of incurring civilian risk, damage, and casualties will be de facto. “Sanitizing” the impact of cyber weapons once they are used by trying to constrain targeting choices will not work.

The anti-LOAC camp makes the same mistake when discussing why the law of armed conflict does not bring clarity to cyberwar:

> The laws of war are in place to ensure that parties to a conflict target combatants rather than civilians, and, if civilians are targeted, to ensure that such individuals have forfeited their protected status. To determine whether cyber-attacks properly distinguish between civilian and military targets, one must understand [the] distinction.[23]

The opposition camp fails in the belief that such a distinction can in fact be created in the cyber realm. This camp does not see the strategic influence of the ambiguity assertion, focusing rather on the deficiencies within LOAC and other contemporary norms and treaties: in short, make better laws and the cyber world will come to heel. As such, this camp is even further from cyber reality, ignoring a problem that is only going to deepen and intensify over time. The opposition camp, in essence, is a more liberal approach to conflict because the end goal is to create an atmosphere of trust that can minimize higher levels of violence and treachery.[24] This flies even more in the face of the current and future structure of cyberwar.

Both of these camps believe in being able to monitor and regulate and circumscribe cyberwar after it has begun, as happens successfully with conventional war. This is a false hope. The ability to monitor, regulate, and circumscribe cyber action is best done through strategy that can inculcate preemptive fear and thereby induce caution and hesitation. Current conventional strategies that aim for trust, target distinction, and minimizing noncombatant impact are simply inexplicably ignoring how cyberwar is organized, structured, and operationalized.

Liberal thinking also dominates the legal community, which is heavily leaned upon for law projects and the strategic thinking that purportedly infuses said projects for the cyber domain:

> [An effective solution to the global challenge of cyber attacks] cannot be achieved by individual states acting alone. It will require global cooperation. We therefore outlined the key elements of the cyber treaty – namely, codifying clear definitions of cyber warfare and cyber-attack and providing guidelines for international cooperation on evidence collection and criminal prosecution – that would provide a more comprehensive and long-term solution to the emerging threat of cyber-attacks.[25]

The only thing left to add here is to note yet another camp focusing on mitigating risk and limiting damage in the cyber domain ex post facto. Regardless of philosophical standing, political agendas, or theoretical acumen, every camp that examines the problem of parameters and definitions in the cyber domain seems to exclude considerations of preemptive strategies built upon fear and inducing reluctance to action. General Alexander of US Cyber Command cited the need to establish the lanes of the road for what governments can and cannot pursue and asserted that establishing those lanes was the necessary first step to addressing the challenge of cyber attacks.[26] What all of the camps examined here have in common is a tendency to give lip-service to strategy, but then really focus exclusively on ex post facto operations to establish progress. If the focus continues to be on agency action rather than on structural deficiency, then progress will not simply remain slow: it will become non-existent.

Duqu's Dilemma: Why It Matters

This analysis has pinpointed flaws in the current thinking and efforts to establish clear definitions and parameters governing the rules and operations within cyberwar. The emphasis placed here on inherent structural difficulties, namely, the innate cyber civilian/military fusion, has shown the likely damaging and deadly consequences to societies when strategies do not focus on the effort to stop cyber action preemptively, focusing instead on operational considerations after conflict has begun.

Only now are isolated legal analyses highlighting these problems beginning to emerge:

> It is unlikely that a state such as the United States could take precautions against the effect of attacks on military objectives by separating military objectives from civilians and civilian objects in cyberspace. This is because of the interconnectedness of US government and civilian systems in the near complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities... Proportionality assessments likely will prove particularly precarious in cyberspace, where outcomes are more difficult to predict than in the physical world: physical attacks at least have the advantage of physics and chemistry to work with. Because, say, the blast radius of a thousand pound bomb is fairly well understood, one can predict what definitely lies outside the blast radius and what definitely lies inside. Error bands and cyber-attacks are much wider and less well-known... [Most reports do not explain how] these public-private partnerships could be constituted in a manner that adequately considers laws of war issues nor do [they] address the likely use of active defenses by the private sector.[27]

As illustrated above, this structural issue is more than just semantics. It literally covers who engages cyberwar, what can be destroyed in cyberwar, who can be a victim during cyberwar, even the philosophical and ethical questions meant to be asked about cyberwar itself. Duqu's Dilemma is an entreaty to move away from unattainable goals and idealistic dreams in a futile hope to create sanitized cyberwar. Cyberwar will never be sanitized. Consequently, contemporary strategic thinking about the cyber domain must start treating the ambiguity assertion with the same gravity that the more famous attribution problem receives.

Notes

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict," *Cybersecurity Policy Report*, February 14, 2011.

2 Tom Gjelten, "Shadow Wars: Debating Cyber Disarmament," *World Affairs* 173, no. 4 (2010): 33-42.

3 Ibid.

4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar," *National* Journal, June 10, 2011.

5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory," *European Conference on Information Warfare and Security* 177-XI (July 2010).

6 Vida Anatolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?" *Naval Law Review* 51, no. 132 (2005): 1-34.

7 Don Tennant, "The Fog of (CYBER) War," *Computerworld* 43, April 27, 2009, pp. 28, 30-32.

8 James Fallows, "Cyber Warriors," *Atlantic Monthly* 305 (March 2010): 58-60, 62-63.

9 Ibid.

10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials Say," *Cybersecurity Policy* Report, March 26, 2012.

11 Lolita Baldor, "Cyber Warriors," *Army Times*, August 6, 2012, p. 23.

12 Siobhan Gorman and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack," *The Australian,* June 1, 2011.

13 Anonymous, "Military Ponders Cyberwar Rules," *Los Angeles* Times, April 7, 2008.

14 Ellen Nakashima, "Pentagon Seeks to Expand Rules of Engagement in Cyber War," *Washington Post*, August 10, 2012.

15 Ibid.

16 Ellen Nakashima, "Cyber Offense Part of Strategy," *Washington Post*, November 16, 2011.

17 Wesley Andrues, "What US Cyber Command Must Do," *Joint Forces Quarterly* JFQ 59 (Fourth Quarter 2010): 115-20.

18 Ibid.

[19] Ibid., p. 120.

[20] Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011): 81-99.

[21] Ibid., p. 90.

[22] Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review* 68 (2012): 167-206.

[23] Michael Gervais, "Cyber Attacks and the Laws of War," *Journal of Law and Cyber Warfare* 30, no. 2 (2012): 525-79.

[24] Ibid., p. 561.

[25] Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review, Inc* (2012): 817-85.

[26] Ibid., p. 884.

[27] Hannah Lobel, "Cyberwar Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas International Law Journal* 47, no. 3 (2012): 617-40.

The Strategic Uses of Ambiguity in Cyberspace

Martin C. Libicki

Strategic ambiguity has an honored place in the mores of statecraft. The studied unwillingness of states to say what they have done (or would do) coupled with the lack of proof that they have done it (or would do it) liberates other states. They can argue that something was done, but if their purposes so dictate, they can pretend that it was not done. The degree of doubt can vary: from thorough (no one is sure what has happened or would happen) to nominal (no one is fooled). In either case, however, those who did it have provided a fig leaf, however translucent, that other states can adopt.

Examples of Strategic Ambiguity in Physical Space

One time-honored example is Israel's refusal to admit (or deny) that it has nuclear weapons. No reputable analyst believes that Israel does not have nuclear weapons. But since Israel has never announced whether it has any, other states are free to pretend that Israel has not crossed the nuclear barrier. This is convenient for states that would be pressured by their people to respond with nuclear programs of their own were Israel's status overt. It also helps states that could not ship certain classes of exports to Israel were Israel's status more open.[1] At the same time, no sane country behaves as if Israel lacked a nuclear retaliation capability.

A parallel ambiguity concerns the putative US use of Predator attack flights and cruise missiles against al-Qaeda members in countries such as Yemen or Pakistan. Official policy is to deny that such flights take place. When Yemen's leader claimed that these were Yemenite operations, very few analysts were fooled. But at least until recently, the leaders of these countries did not have to contend with admitting that sovereignty violations were taking place, with at least their tacit permission.

Dr. Martin C. Libicki is a Senior Management Scientist at the RAND Corporation.

This article was first published in *Military and Strategic Affairs* 3, no. 3 (2011): 3-10.

Another longstanding example is US policy towards Taiwan's independence. The United States has declared both that it opposes a Taiwanese declaration of independence and any attempt to resolve the status of Taiwan by force. The United States does not recognize Taiwan as a state and so has no mutual aid pact with it. However, if Taiwan declared independence and China decided to take the island, would the United States intervene on Taiwan's side? It is clearly in the US interest for China to think so in order that China does not start a war. But it is almost as clearly in the US interest for Taiwan to think otherwise, so that Taiwan does not provoke China into starting a war. Assume the odds of a US intervention are literally a coin toss and perceived that way on both sides of the Straits. If so, Taiwan may well calculate that the expected value from declaring independence is negative (whereas it would have been positive if the US were definitely coming to help), due to the fact that the United States might decide not to intervene. Similarly, China could conclude that the expected value of a cross-Straits invasion is also negative because the United States might intervent. Anything less ambiguous could well prompt one or the other to do something foolish.

Cyberspace is Tailor-Made for Ambiguity

Cyberwar is, literally, inside work. When hackers enter a computer system to misdirect its workings, the direct results are often literally invisible to the outside world. Depending on how such systems have been misdirected, the indirect results may be invisible as well. True, the results of a cyber attack on a power grid that turns off the lights can be viewed even from space. But without further investigation and revelation, it will not be clear whether a blackout was a deliberate attack, or the result of human error, bad software, or (most frequently) Mother Nature. Even if it were clear that a system misbehaved because it had been attacked, exactly who attacked may be shrouded in mystery. Finally, even if the fact and the author of the cyber attack were clear, the purpose may be quite obscure: after all, cyberwar alone cannot kill anyone, or even break very much (but see Stuxnet), much less seize territory or change a regime (and whereas cyberwar can facilitate other applications of force, it is those other applications that are more visible). Nearly all intrusions are meant to steal information or "rent" the capacities of the target machine (as in a bot) and otherwise leave the system alone. Deliberate attacks can often be framed as attempts to mislead people (e.g., false radar images) or their equipment (see Stuxnet). In the latter cases, obviousness is self-defeating; once it is clear that you have successfully deceived a system, the system's administrators are unlikely to allow the system to operate as it has.

Is Stuxnet an Exception?

One would imagine that a cyber attack that actually broke something might have passed the point where everyone could be try to hide its existence. The Stuxnet worm was discovered in June, 2010, and its target was identified as an Iranian nuclear facility in September. The earliest suspicions tagged the Bushehr reactor as its target,[2] and the Iranians denied that any such reactor was affected. Within a few weeks, the Natanz centrifuge plant was identified (more plausibly) as its target. Initial Iranian denials were contradicted in late November, 2010, the day that assassins killed two Iranian nuclear scientists, and when Ahmadinejad admitted that there was a worm that had caused a great deal of trouble, which was then taken care of.[3] How badly did Stuxnet, in fact, hurt Iran's nuclear development? Statistics from the IAEA would indicate that it may have led to the premature retirement of 10 percent of Iran's centrifuges and thus, at most, it bought the worm's creators several months reprieve from the data at which Iran would have enough nuclear material to build its first bomb.[4] Other reports quote officials predicting that the earliest that Iran can (as of early 2011) assemble such material would be 2015, a delay of several years.

There is a lot more (apart from what it accomplished) that is currently unclear about Stuxnet.[5] One question is how it got into Natanz in the first place; suspicions that the worm's designers received witting or unwitting help from Russian contractors appears to have soured Iran's working relationship with them.[6] More important is exactly who wrote and released the worm. Was it an individual (its sophistication says otherwise)? Was it Israelis – as suggested by several clues internal to the code – but who knows that these clues were not planted to mislead suspicion? Was it Americans? Was it both, working together?[7] Or, was it the Chinese?[8] With all the ambiguity, it is no wonder that Iran has yet to retaliate (at least in any noticeable way). That noted, Syria did not respond to the strike on its suspected nuclear facility, and Iraq did nothing but complain when its Osiraq reactor was bombed – and there was no ambiguity who did it in both cases. Conversely, Iran's strong ties to Hamas and Hizbollah suggest that it may have had ways of expressing its displeasure that were unavailable to Syria (in 2007) or Iraq (in 1981). Furthermore, Iran has yet to make much of a big deal about the incident; likening it to an act of war after months of silence and denials would be quite a volte-face.

The advantages of using Stuxnet rather than airpower to degrade Iran's nuclear capability are fairly clear (assuming the worm, in fact, did as its designers hoped): comparable effect, and induced distrust among its victims as to which of its suppliers or supplies may still be contaminated, but with less condemnation (indeed, perhaps a sneaking admiration) and fewer strategic risks.

The Uses of Ambiguity

The working hypothesis is that a cyber attack used in lieu of kinetic methods creates more ambiguity in terms of effects, sources, and motives. Thus, if cyber attacks work – and this is a tremendous if – they change the risk profile of certain actions, and usually in ways that make them more attractive options. What follows are some hypothetical uses of cyber attacks.

One, cyber attacks may be used by a victim of small scale aggression to indicate its displeasure but with less risk of escalation than a physical response would entail. In late 2010, for instance, North Korean forces shelled a South Korean island, killing two civilians and two service members. A retaliatory cyber attack that disrupted an important industrial facility (ignoring the fact that North Korea is not well digitized and has nearly zero network connections to the rest of the world) could have conveyed displeasure. North Korea, if it wanted to respond, would have had to (1) admit that one of its facilities had been hacked, and (2) take steps to indicate why it was South Korea, and only South Korea that was at fault (it could be the United States or even Japan, and China). Conversely, if North Korea did not react publicly, it stood a good chance of limiting the number of people with a good idea of why some facility ceased working. This introduces another advantage of cyber warfare over physical combat: although being attacked may be a source of pride (e.g., you can play David to the enemy's Goliath), being hacked primarily means that you ventured into cyberspace with inadequate attention to maintaining control over your systems. Victimhood is not something worth boasting about. Thus, states that can hide having been attacked may well do so, thereby saving face – but doing so also making an obvious response less likely. They could, of course, respond in kind and so a tit-for-tat struggle that started in the physical worlds ascends (or descends) into the virtual one. But that course may be safer all around than coming to blows.

Two, a state rich in cyber warriors may also use the threat of cyberwar to deter the potential target against support proxy war fighters: e.g., Israel could threaten Iran with cyber attacks if Israel is attacked by Hizbollah, a group with known links to Iran.[9] In this situation, Israel may not want to make such a threat public. A public threat would allow Hizbollah to coerce Iran by claiming a desire to wreak the sort of mischief that would prompt Israel to strike Iran in cyberspace. But there are private ways to convey the threat, and such a threat has logic. The usual problem with cyber deterrence is that attribution (of the starting attack) is a problem, but a physical attack – say, Hizbollah rockets striking Israel – would be obvious. Conversely, although a state like Iran may not fear a direct Israeli attack even in response to a Hizbollah attack (no such attack materialized in 2006, for instance), it may fear a cyber attack given the clear superiority of Israeli hackers over Iranian ones. Such superiority mitigates (although it does not erase) the fear that having declared the intention to carry out a cyber attack, Israel would have no accessible targets in Iran; even if the success of any one attack is uncertain, the odds that enough will succeed and hurt are sufficiently good. Iran's blaming the United States afterwards may be a problem for the United States but make things easier for Israel. Escalation into violence is not really an option for Iran given Israel's conventional combat dominance (at least if the battle were close to Israel). More to the point, Iran would have to admit its systems had been conned and make a convincing case that it knew who did it. Finally, while Israel is more wired than Iran, again, with Israel's cyber capabilities, that fact may not be enough to turn the tide towards Iran's favor should it strike back.

Three, cyber attacks can be used by one state to affect the outcome of conflict in another state without having to make any sort of visible commitment, even an implied one. Consider the civil war in Libya. If Libya's military was sufficiently wired so that cyber attacks could conceivably make a difference in its capabilities,[10] then Western hackers, by disabling the central government's forces, could conceivably tilt the direction of the fight. If the rebels won, Western governments would be better off as a result. Rebel forces, at worst, would have no way of knowing they had received assistance, and that may be just as well (particularly regarding the more jihadist of Libya's rebels who greet the intervention of US forces by switching sides). Or, hints could be offered (e.g.: if this capability fails tomorrow, you will know why). Conversely, if the government won, it may suspect that its information systems were tampered with by Western forces, but it may not be able to prove as much. It may complain, but if Libya were expected to blame its shortfalls on the West, then such complaints, in the absence of evidence, would have little force. More to the point, it may not want to claim as much if it wants to pretend afterwards that it has no reason to make enemies of the West all over again. If the civil war drags on, the West can pretend that it had made no prior help and thus had made no commitment to escalate its assistance (even if hints were dropped to the rebels, they would have an even harder time proving to others that Western hackers were offering assistance, since unlike the government, they would likely have no access to the tampered computers). The greatest problem in offering such assistance is the possibility of getting caught, but if the target of the attacks is on the outs with the rest of the world, it is unlikely that it will get much help tracing the attacks. So attractive is such assistance (at least from the helper's perspective) that it may be a routine feature – on both sides – of any conflict where the outcome is uncertain and networks matter to war fighting capabilities. And again, admitting that one's systems have been hacked is always at least a little embarrassing.

Four, cyber attacks do not need to be directed towards adversaries, although the risks of making new enemies if the source of the cyber attacks are discovered are obvious. Consider a situation in which two neutral states are inching towards war that one might prefer not take place. Suppose that a third state is capable of introducing faults into both sides' surveillance and/or command-and-control systems that raise doubts whether they have pierced the fog and overcome the friction enough to undertake military operations. If systems go haywire, either target state is more initially likely to blame the other for its woes (if they understand that such woes were obvious *and* induced rather than non-obvious or accidental) rather than a third party; chances are that the initial presumption is likely to color their forensic activities and conclusions. Furthermore, there is a good chance that such blame will be kept private given the embarrassment involved. Yet risks exist in such maneuvers; such machinations may drive states towards war if one side or both comes to convince itself, for instance, that the cyber attacks from the other side are precursors to an immediate movement of forces, or are indications that their foes' forces are not just posturing.

A variant on this technique is to use cyber attacks to disable a capability in a state whose leadership is reluctant to use it anyway (either because the leadership feels itself to be on shaky political ground vis-à-vis its excitable populace, or because the leadership is exercised by a consensus among factions[11]). Once such a capability is found inoperative, the political leadership announces to its military leaders that it has no option but to stand down. Perhaps the military unearths evidence that a third party was behind such an incapacity – the political leadership, relieved at not having to act, may deem such evidence inconclusive or not credible it in the first place.

Five, ambiguity may be useful in declaratory policy, one that indicates how a state would respond to a cyber attack. Ambiguity has both costs and benefits. The cost is that others may think they can get away with attacks that they would have forborne if they had understood that reprisals would follow. But the benefit is that the target state may not want to strike back, particularly if it lacks the confidence to attribute the attack. A state that fails to strike back because it is unsure may not lose stature in its own eyes – attribution really is difficult. Yet if the attacker (and others) come to believe that such a state *did* know but pretended otherwise for fear of a full-scale fight, then any threat to retaliate rings hollow – and not just in cyberspace. If a state leans too far forward in promising reprisals in response to cyber attacks and cannot deliver, its ability to deliver against all other threats may be further doubted.

Conclusion

Cyberwar's many tactical ambiguities lend force to a strategy built on strategic ambiguities. There may be many cases in which an aggressor state does not want what it has done it to be obvious. Even the target state in some cases may conclude that pretending as much (even if it must turn a blind eye to the evidence) has advantages over trying to clarify matters or even claiming clarity in absence of the real thing.

But the downside to strategic ambiguity should be noted. States may arrogate the right to carry out all sorts of mischief in cyberspace on the belief that they will never be called into account. The lack of accountability, however, is inherently dangerous. Sometimes it is unwarranted (the state is only fooling itself), and even if warranted, it provides hackers a degree of freedom that history suggests is dangerous in and of itself.

Notes

[1] By contrast, legislation had to be passed in 2006 to permit the United States to share civilian technology with India, which like Israel is a non-signatory to the Non-Proliferation Treaty, but unlike Israel, a declared nuclear power. See Peter Baker, "Signs India Nuclear Law: Critics Say Deal to Share Civilian Technology Could Spark Arms Race," *Washington Post*, December 19, 2006, www.washingtonpost.com/wp-dyn/content/article/2006/12/18/AR2006121800233.html.

[2] Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?" IDG News, taken from *PCWorld*, September 21, 2010.

[3] William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientist," *New York Times*, November 30, 2010.

[4] Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *Washington Post,* February 16, 2011. See also the report by the Institute for Science and International Security, http://media.washingtonpost.com/wp-srv/world/documents/stuxnet_update_15Feb2011.pdf.

[5] What *is* most clear about Stuxnet is how it worked because the worm was captured alive, so to speak, in the wild before it could self-destruct (which it should have done if it was unable to find a specific programmable logic device that met certain preset parameters associated with a particular type of centrifuge).

[6] "The Stuxnet Worm: A Cyber-Missile Aimed at Iran?" *Economist*, September 24, 2010, www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

[7] William Broad, John Markoff, David Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

[8] Jeffrey Carr, "Stuxnet's Finnish-Chinese Connection," December 14, 2010, blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/.

[9] Many observers take issue with the characterization of Hizbollah as a puppet of Iran. Yet there is a difference between Hizbollah acting only on Iran's orders, and Iran having enough influence on Hizbollah to discourage it from unwise actions.

[10] An influential article reviewing the possibilities of Western intervention in Libya mentioned electronic warfare in the form of communications jamming, but nothing about cyber warfare. See Thom Shanker, "U.S. Weighs Options, on Air and Sea," *New York Times*, March 6, 2011, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

[11] If the fact that China's stealth fighter surprised Hu Jintao when meeting with Secretary of Defense Gates is any indication, its military is not absolutely beholden to its political leadership and thus the country's effective leadership may also be somewhat of a coalition.

An Interdisciplinary Look at Security Challenges in the Information Age

Isaac Ben-Israel and Lior Tabansky

Introduction

Developments in electronics and computers since World War II have affected a broad range of fields and created the "information age." This article focuses on interrelationships among information technology, the information age, and security. More specifically, it aims to contribute to a discussion of the national security issues stemming from the development of information technology.

Much of the driving force behind computer development has been derived from military applications. Following new possibilities, thinking about the effect of technological change on defense issues has also progressed. In addition, the information age, which continues to develop rapidly, along with advances in computer communications and the penetration of computers into every area of life, has given rise to cyberspace. These developments challenge existing perceptions and force reconsideration of basic concepts. The need for an informed public debate and the design of a firm policy has likewise grown, given the fact that the cyberspace risk is already concrete – as dramatized by events in Estonia in the spring of 2007, as well as the Stuxnet affair.[1] In Estonia, daily life was disrupted following a technically simple but massive attack on internet-based services. With Stuxnet, it appears that a technically complex cyber weapon was used, designed to cause precise damage to the system controlling the industrial process at a protected nuclear fuel enrichment facility in Iran. The weapon's design and method of operation included camouflage of its activity for

Prof. Isaac Ben-Israel is head of the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University. Lior Tabansky is a Neubauer research associate working on the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation.

This article was first published in *Military and Strategic Affairs* 3, no. 3 (2011): 21-37.

a prolonged period. This cyber weapon apparently caused cumulative physical damage of strategic significance. The consensus is that in both incidents, states were behind the cyber attacks, though in both cases no definitive evidence exists.

A basic theoretical understanding of the information age is essential in order to consider cyber security issues. This article relies on ideas by philosopher Karl Popper, futurists Alvin and Heidi Toffler, and economist Paul Romer to illuminate the characteristics of the information age and to clarify the issues that emerge when technological development interfaces with national security. It analyzes the current characteristics of cyberspace, and discusses the implications for national security questions. It then reviews the field known as information warfare and focuses on the totally new phenomenon of computer warfare in cyberspace. The article then reviews cyber weapons and methods of warfare, discusses defense, attack, and deterrence, and presents key issues in the cyber defense realm. It appears that in order to maintain security and peace, a multidisciplinary assessment of the new issues and challenges is required.

Theoretical Background

Technological change occupies many thinkers who struggle to assess its social effects. Although the scope of this article does not permit a full review of the field, three thinkers relevant to an understanding of the dynamic reality must be mentioned.

The term "Third Wave," taken from the theories of the bestselling authors Alvin and Heidi Toffler, refers to a time period (table 1). According to the Tofflers, we are in the midst of a transition to the Third Wave, in which the economy is based on knowledge and control of information,[2] instead of on industrial mass production. Similarly, the form of warfare is changing as well. The name of the game has become obtaining information about the enemy and denying it information about yourself. The side that controls information technologies will win the war, even if it faces many weapons rolling off Second Wave assembly lines.

Table 1. The Waves According to the Tofflers

	Principal Resource	Who is Rich	Symbol	Weapons	Method of Waging War
The First Wave	Organized agriculture	Landowner	Sickle	Sword	Face-to-face battle at point blank range; land conquest
The Second Wave – from the mid-17th century until the end of the 20th century	Automated industry, mass production	Industrialist	Machinery of mass production assembly lines	Tank, airplane	Machines used at medium range, poor accuracy, attempt to damage production capacity
The Third Wave – from the end of the 20th century onwards	Knowledge	Bill Gates	Computer	Cyber warfare	Attempt to damage information through the use of computers. Remote damage to functional capacity, without physically reaching the target

Concepts developed by philosopher Karl Popper, who died in 1994, enhance the theoretical stage. Popper analyzed the world of knowledge as another existing concept, in addition to the material and spiritual worlds (table 2).[3] Popper insists that an entire "world" of human knowledge exists (World 3), populated by "beings" that are objective contents of thought, such as the Pythagorean Theorem and the laws of physics. These are neither "material" nor subjective "mental experiences." Once the Pythagorean Theorem was formulated, it became an objective truth independent of the spirit that created (or discovered) it. In other words, knowledge is objective, even though it is a product of the (subjective) human spirit.

Table 2. Popper's Three Worlds and Cyberspace

	Contents	Status	Examples	Example in Cyberspace
World 1	Material	Objective	Tables, airplanes	Hardware
World 2	Mental experiences	Subjective	Pain, happiness	Displays (the user experience)
World 3	Knowledge	Objective	Mathematics, physics	Software

Unlike material, knowledge can be used again and again and shared with many consumers without being diminished. Knowledge or information is a non-rival, partially excludable good. Paul Romer, a pioneer researcher in the new theory of economic growth, discusses the economic consequences of knowledge, and lays the foundations for a "different" knowledge-based economy.[4] He argues that growth in the economy, the basis of power and prosperity, is not solely a result of changes in capital and manpower. The development of knowledge is a new, potent source of endogenous growth. The character of this knowledge-based growth differs from what is familiar in the traditional economy.

If we combine Popper's metaphysical basis with Toffler's sociology and Romer's economic theory, we can suggest that the wars of the First and Second Wave were conducted mainly in World 1 ("material"). In these wars, the side with the largest and strongest army that was best able to mobilize troops and develop the mental factors (World 2) among its troops (e.g. the spirit of battle, motivation, and courage) would be victorious. According to this theory, future wars will also spread to World 3, the world of information. Without derogating the value of these elements in the future, while past wars relied on physical force (the First Wave) and present wars rely on the power of machinery (the Second Wave), future wars will rely more and more on brainpower.

Intellectual Approaches to National Security in the Information Age

The outstanding symbol of the information age – the electronic computer – was built at the end of WWII to help the US military in artillery ballistic calculations. In the decades following, especially after the invention of the transistor and the integrated circuit, computers have continually shrunk in size. Gordon Moore, co-founder of computer processors manufacturer Intel, stated in 1965 that the number of transistors that could be placed on an integrated circuit would double every 1-2 years, while the price would remain constant.[5] When this rule proved valid for semiconductors, the prediction was dubbed "Moore's Law." Futurist Ray Kurzweil presents persuasive arguments for extending Moore's Law to information technologies in general.[6]

With the development of the computer and its shrinking physical dimensions, defense institutions employ computing to improve the performance of many systems. The chief benefit was a revolution in the accuracy of munitions, manifested first in airpower. Computers initially contributed to better operational planning. When it became possible to install a computer in warplanes, the power of computing was harnessed for the purpose of attack missions. An important strategic change occurred when the computer's dimensions and price were downsized enough that it could be embedded in ammunition itself. Thus was born the era of "smart weapons" – precision guided munitions that were initially adopted in aerial warfare. The operational results were stunning. In an attack on a specific individual target, such as a tank, one airplane armed with smart weapons can now do what 15 airplanes could do 30 years ago, or what 60 airplanes could do 40 years ago.[7] No wonder this technological revolution has had a decisive effect on the theory of warfare.

In order to adapt the art of war to information technology, a new theory of warfare dubbed "the Revolution in Military Affairs" (RMA) was developed in the early 1990s, based on four fundamental elements: precision strike, space power, dominant maneuver, and information warfare.[8] Information warfare involves several different aspects: computer warfare (computers are the main technological means of storing and transporting information), electronic warfare (mostly against sensors and communications systems), psychological warfare and managing the media (media briefings, embedding reporters in combat units, and manipulation of the information released to the public). These terms must be used accurately and the meaning of "information warfare" must be fully understood, particularly as these concepts have evolved with the advent and development of cyberspace.

The direct result of RMA is the absolute military superiority of the developed countries on the battlefield,[9] as reflected in the US wars in Iraq and Afghanistan, and in Israel's wars in Lebanon and against terrorist organizations. Indeed, a critical benefit of RMA is the unprecedented capability to conduct accurate and effective low intensity warfare, and the ability to defeat terrorism through military means, without causing widespread collateral damage.[10] As computer development continues, however, a change in approach is required. What follows is intended to provide a basis for an updated concept of national security in a reality that includes the new cyberspace.

Cyberspace

The ongoing growth of computers and communications networks generated a new situation at the beginning of the 21st century: an additional computerized layer above the existing older systems that effectively controls their function. The spread of computers, their integration in various devices, and their connectivity to communications networks have created a new space. Cyberspace is composed of all the computerized networks in the world, as well as of all computerized end points, including telecommunications networks, special purpose networks, the internet, computer systems, and computer-based systems. The concept also includes the information stored, processed, and transmitted on the devices and between these networks.[11] This picture enables us to understand what is happening in World 3[12] while focusing on the encounter with national security issues.

Unlike land, sea, air, outer space, and the electromagnetic spectrum, cyberspace is not a product of nature. Cyberspace is created by human beings, and would not exist without the information technologies developed in recent decades. Knowledge – which is perhaps the most important element in cyberspace – is a product of cumulative human endeavor.[13] The structure and design of cyberspace as it is today has significant consequences for national security (table 3).[14]

Table 3. Characteristics of Cyberspace and their Weak Points

Characteristic	Weak Point
Rapid change	Rapid obsolescence of means, including defense systems
TCP/IP protocol architecture	It is difficult to track the signal in the network and attribute it to a source.
High level of complexity	It is very difficult to connect an event to its cause, and difficult to distinguish a malfunction from an attack.
Extensive use of standard commercial off-the-shelf equipment	A narrowing gap between small and large players. The vulnerability of identical hardware and operating systems puts a broad range of systems at risk.
Entry-level cyber weapons are relatively cheap	The scope and price of defense is increasing.
An unclear legal environment	A gray area with a low probability of punishment encourages instability.

Cyberspace can be described as consisting of three layers.[15]

a. The most tangible layer, which currently provides the infrastructure of the computer world, is the physical layer. The physical components are the concrete building blocks of cyberspace – building blocks with natural characteristics: width, height, depth, weight, and volume.[16] In Popper's theory, the material layer corresponds to World 1.

b. The second layer is software logic, a variety of command systems programmed by people, intended to instruct a computing device. The physical components are controlled to a large extent by software, and the information stored on computers can be processed through software commands. The software layer is partly physical (World 1) and partly logical, meaning, again, World 3.

c. The third layer of cyberspace is the data layer that a machine contains and processes. The data and its processing generate information and knowledge. This layer is the least tangible of the three, mainly because the characteristics of information are very different from objective physical characteristics. This layer definitely belongs to Popper's World 3.

From Information Warfare to Cyber Warfare

In American and European professional literature,[17] information warfare is considered a significant feature of the information age. In American military terminology, information warfare is called "information operations," and its computerized component is called "computer network operations" (CNO).[18]

Table 4. Topics Included in Information Warfare

Topic	Relevant Systems and Technologies
Information collection	Various sensors in all parts of the electromagnetic spectrum
Transporting information for processing and the consumer	Broadband communications, compression, encoding, encryption
Storage and retrieval	Databases, de-duplication, compression
Processing and filtering information	Digital signal processing (DSP), automatic target recognition (ATR), data fusion, artificial intelligence (AI)
Making information accessible	Broadband communications, display systems, and a human-machine interface
Denial of information	Jamming, electronic warfare (EW), encryption, deception, obfuscation
Information protection	Denying unauthorized parties access to your information, encryption

Table 4 shows that the topics listed under information warfare are actually "classic" topics existing throughout the history of war. In the course of history, several classic methods of warfare have been developed for "information warfare," including intelligence gathering by human "sensors" (as in Joshua's use of spies in the conquest of the Promised Land) and the development of special gathering technologies (such as airborne intelligence sensors, satellites, etc.). Classic methods have also been developed in the prevention aspect of information warfare, such as camouflage, dummies and masks, jamming and blocking, deception and misdirection, propaganda, and so on.

Further analysis of table 4 indicates that the increasing dependence of information systems on computing is practically the only innovation in this field. In other words, while information warfare is not new, this is not true of computer-based information systems. Cyberspace makes it possible to define new targets, weapons, and methods of warfare. What is new about Third Wave warfare or war in the information age is not information warfare per se, but computer warfare. For this reason, it is best to limit the discussion by focusing on computer warfare in cyberspace. The change in cyberspace is so great that the basic concepts, such as "war," "weapon," "attack," and "defense," require a new explanation.

Computer warfare in cyberspace is unauthorized access to the adversary's computer systems for the purpose of intelligence gathering, disruption, deception, and prevention and delay of the use of information, while preventing the enemy from doing the same to one's own computer systems. A traditional attack (barrage, bombing, physical sabotage) on computer systems will also certainly cause disruption, prevention, and delay in the use of information. Such a physical attack, however, is not classified as cyberwar.

The characteristics of cyberspace[19] also define warfare in this sphere. The characteristics of cyberspace make it difficult to distinguish between a deliberate attack and malfunction, and complicate the effort to attribute action to a specific party, thereby also making it difficult to respond to an attack. The characteristics of cyberspace today empower marginal players, and give the attacker an advantage over the defender.

In recent years, a discussion has developed about the vulnerability created by the indispensability of cyberspace in all life processes in a developed society.[20] Computer warfare is not confined to military systems;

with the spread of computers and communications networks, it has become applicable to all areas of life. Most systems in the civilian economy and the entire critical infrastructure are now dependent on computers, and are part of cyberspace. This fact generates vulnerability and new possibilities for warfare, and also requires defensive preparation in developed countries.

Attack and Defense in Cyberspace

Cyber weapons[21] are malware and harmful hardware that damage the victim's computer resources and disrupt his data, deceive, and cause deprivation of service or the collection and transfer of intelligence. "Malware" is hostile software designed to disrupt orderly activity of a computer system and damage the process managed by that system. "Spyware" is hostile software designed for covert data collection and its potential transmission over a network. "Phishing" is a stratagem based on software and social engineering designed to fraudulently obtain personal data and details of user identities to gain unauthorized access to sensitive resources.

Hardware can be implanted through the addition of an electronic component to an existing unit, or an addition within an integrated circuit. The implant can take place during manufacture, transportation, operation and maintenance.[22] The use of software as a logical weapon, more common than the use of hardware, is what enables the most advanced methods of warfare. Knowledge and technology are non-rival, partially excludable goods; these inexhaustible characteristics make them hugely important in all matters pertaining to information warfare. Not all the consequences of this potential have been fully clarified.[23]

When there are good grounds to suspect that a cyber attack is underway, it is very difficult to identify the source and the attacker's identity. All parties operating in cyberspace use common tools and methods. Commercial cooperation, a kind of outsourcing, frequently takes place between the technical parties possessing attack capabilities (programmers, encoding hackers, owners of "captive networks") and those ordering the services (private investigators, organized crime, espionage organizations). In order to determine that a cyber attack is an act of war, several aspects must be examined:

a. The organizational and geographic source: whether a state is behind the action[24]

b. Motive: whether it is possible to identify an ideological, political, economic, or religious motive for the attack
c. Level of complexity: whether the attack required complex planning and coordinated resources that are available primarily to state agencies
d. Results: whether the attack caused damage and casualties, and whether it would have caused damage without the defensive actions taken.

The characteristics of cyberspace make it difficult to answer these questions, and answers sufficient for setting policy will undoubtedly be lacking.

For adequate defense, it is necessary to discern there is an attack, which is no simple matter in cyberspace. Early implantation of malicious hardware or software, especially before testing plans have been formulated, reduces the chances of detection. More accurate cyber weapons cause little collateral damage, which makes detection of the attack by the victim less likely. Defensive actions involve three aspects:[25]

a. Detection: the Achilles' heel – how to realize that a computer attack has taken place
b. Prevention: a means of stopping the attacker at the penetration stage
c. Response: recovery measures to limit the attacker's achievements, forensic means, and even retaliatory action.

Key Issues in Cyberwar

The technological change underlying the transition to the Third Wave, the rapid expansion of World 3, and the development of the information economy raise new questions. One of the most important is the debate on critical infrastructure protection. The feasibility of a cyber threat to the infrastructure of a modern society was presented through experiments, such as a power generator being put out of action and blown up by broadcasting commands to its command and control system.[26] It appears that this threat became a reality in the summer of 2010, when the Stuxnet worm virus that infected "Windows"-based computers was discovered. It searched for computers running Siemens-produced industrial command and control software of a certain type connected to an industrial controller of a specific model. Only if it located the relevant computers, the virus activated software code that disrupted the activity of the computerized controller, while concealing the change from the control software and equipment operators. Stuxnet allegedly damaged the proper operation of the centrifuges for uranium enrichment in Iran. The source and duration of the attack are unknown.[27]

The US, the world's only superpower, is a pioneer and leader in the discussion of its cyber vulnerability.[28] A country's critical infrastructure is an obvious target in any conflict. Nonetheless, why has such concern been raised now, and in the strongest countries? The answer lies in the transition from the wars of Toffler's Second Wave to the wars of the Third Wave, the information wave. Discussion of critical infrastructure protection has been renewed because of the emergence of a new threat that could not have been carried out before. The development of cyberspace makes it possible, for the first time in history, to attack critical infrastructure systems in cyberspace, without physical access to the site and without exposure during or after the attack.

Critical infrastructure protection is one of the key issues of cyber security. The topic is outside the scope of this study, and deserves a specific discussion of its own.[29]

"Information warfare" immediately invites examination of the concept of war itself: is a cyber attack on computerized information involving no use of firepower an act of war? What constitutes a legitimate target in such a war? The extensive military use of civilian infrastructure (mainly communications) complicates the distinction between military and civilian targets. For example, the computer infrastructure of the US Department of Defense consists of 15,000 networks and seven million facilities dispersed all over the world. Most of the US Defense Department communications, however, are channeled through commercial civilian networks.[30] Civilians (even women and children) can be as effective as soldiers in computer warfare. Does this make them potential targets of a response? How should we act in a case of widespread economic damage? Moreover, the meaning of such an attack is unclear. Assume that one day the computer systems of the Israeli banks crash. Assume also that we manage to determine with certainty that the enormous damage was caused deliberately by a deliberate penetration, and assume that we succeed in tracing the attacker to the territory of a neighboring country. Now, is this an act of war? Ostensibly, the damage caused is "only" economic; there are no (direct) human casualties. Countries have frequently responded with restraint to traditional attacks that caused economic damage but did not take human life.[31] Economic damage, however, is liable to paralyze an entire country. How do we estimate the indirect damage caused by an attack? Assume that a cyber attack caused prolonged disruption in the supply of electricity. Assume that one of its results is putting road lights and traffic lights out of commission, and the resulting darkness causes fatal traffic accidents. Should a victim of such an accident be considered a cyber warfare casualty? Should we respond with firepower and ground maneuver, or with a cyber counterattack? The problem is more complicated than the scenarios described, because a computer attack does not require a base in a country, and it can also be conducted by organizations and even by individuals.

Computer warfare is also conducted between friendly countries competing for diplomatic and economic intelligence. Is this "warfare?" Is it acceptable or advisable to use computer warfare in peacetime for such purposes?

A special problem in cyber warfare is detecting an attack; in contrast to a traditional attack occurring in World 1, the material world, the location of the strike and the attacker's identity are not necessarily exposed following the attack. There are no defined "front lines" in computer warfare, and geographic distance has almost no meaning in electronic networks. Given the characteristics of cyberspace, detecting an attack cannot be taken for granted: an attack and a malfunction have similar effects. While the computer world has become more sophisticated, as reflected in the multiplicity of software and applications and the growing number of transistors in each component, malfunctions are not less likely. The statistical probability of a software "bug" or programming error is constant, and its nominal value rises with increased complexity of software.[32]

The capability to detect that computers have been attacked and damaged, rather than malfunctioning "naturally," is inadequate. Without the ability to distinguish in real time between an attack and malfunction, large scale investment in constant cyber readiness is necessary. Defense against cyber threats must encompass all aspects of attack and be updated with new developments, and its cost is rising steadily. The argument on difficulty of defense is similar to the argument against an active anti-missile defense and the argument that defense against suicide terrorists is futile. Nevertheless, it is possible to devise a response to the new threats,[33] although the burden is substantial, since the characteristics of today's cyberspace give a clear advantage to attack over defense.[34] The field of encryption is one of the few areas in cyberspace in which the defender still enjoys an advantage over the attacker.[35] Given the difficulty of identifying the fact of an attack, its geographic location, and the identity of the attacker, a state of uncertainty results that makes an escalating response difficult. Table 3 above summarizes the characteristics and many weak points that create the "attribution problem": it is hard to know the attacker's source and identity and on behalf of whom he operated, and it is certainly hard to prove guilt. In the traditional defense realm, great effort is expended on intelligence, advance warning, and deterrence in order to limit as much as possible the resources spent on a state of continual readiness. The problem of deterrence is particularly difficult in cyberspace, mainly because of the attribution problem.[36]

The characteristics of cyberspace give rise to problems for an attacker as well. How can one tell whether the cyber-attacked computers have really been damaged? In order to rely on a cyber attack, battle damage assessment is necessary. From this perspective, an open loop attack, i.e., one whose degree of success is unknown, is of limited utility. This problem is especially acute if the cyber attack was not intended to destroy data but to manipulate it.

In conventional warfare, rules have been developed that are anchored in international conventions. These conventions, which were written before the emergence of cyberspace, deal in "armed conflict," "physical confrontation," "territorial attack," and so on. These concepts are irrelevant to computer warfare, and the existing conventions require adaptation to cyber warfare – Third Wave warfare. Despite widespread research in this field, it is reasonable to assume that an assessment of the issues from a legal standpoint will take many years. The absence of rules makes it difficult to cope on a daily basis with the special problems of cyber warfare. The issues reviewed are not purely legal; they are essential issues for policymaking and taking decisions. In late 2011, NATO was in the midst of formulating a legal framework to enable it to respond to cyber attacks using methods currently of uncertain legality. An understanding of the theoretical foundations of the field is critical for improving the ability to cope with it.

Conclusion

Cyberspace is a fairly new product of the information age, and cyber security is part of the transition to the information age. In order to cope with this challenging change, a multidisciplinary perspective should be adopted. Therefore some of the information age's important theoretical origins were presented, including ideas of the Tofflers, Karl Popper, and

Paul Romer. Clearly there are other sources, and further multidisciplinary research on the information age is welcome.

The problems in dealing with security challenges are a function of the characteristics of cyberspace: rapid action, the rate of change, intricacy, and complexity. Cyber attack and defense take place in World 3, the world of knowledge. The significant consequences of the key issues of cyber warfare described in the last section of this study should be investigated in depth.

The key development is not "information warfare"; it is computer warfare in cyberspace. Discussion of solutions to "computer matters" tends to focus on the technical realm, far away from public debate and public policy. Clearly professional understanding of the field under discussion is essential, and it presents enormous challenges requiring a solution at the national public policy level. However, a review of the main issues of cyber security paints a complicated picture, beyond the technical computer professions. In order to provide national security in the dynamic environment of the information age, it is therefore correct to utilize inputs from every relevant field of knowledge, including the social sciences, psychology, biology, medicine, and philosophy. This study aims to encourage interdisciplinary research into the cyber security challenges, contribute to the development of an informed national security policy, and thereby contribute to security and prosperity in the information age.

Notes

[1] "The Meaning of Stuxnet: A Sophisticated 'Cyber-Missile' Highlights the Potential – and Limitations – of Cyberwar," *Economist (GBR) Economist* 397, no. 8702 (2010), September 30, 2010, from the printed edition.

[2] Information or data is distinguishable from knowledge, which also requires conceptualization and understanding of the raw information. This distinction is unimportant for the purposes of this article.

[3] Karl Popper, *Objective Knowledge: An Evolutionary Approach* (Oxford: Oxford University Press, 1972), chapters 3-4.

[4] Paul M. Romer, "Endogenous Technological Change," *Journal of Political Economy* 86, no. 5, pt. 2 (1990): S71-S102.

[5] E. Mollick, "Establishing Moore's Law," *Annals of the History of Computing, IEEE* 28, no. 3 (2006): 62-75.

[6] Ray Kurzweil, "The Law of Accelerating Returns," (2001).

[7] Isaac Ben-Israel, "From Sword Blade to Computer Memory," *Odyssey 9*, October 2010.

[8] For information on RMA, see: Michael E. O'Hanlon, "Technological Change and the Future of Warfare" (Washington, DC: Brookings Institute Press,

2000); Stuart E. Johnson and Martin C. Libicki, "Dominant Battlespace Knowledge: The Winning Edge" (Washington, DC: National Defense University Press, 1995).

9 This ascendancy has caused the enemy to retreat to a strategy of survival and asymmetric warfare.

10 This capability was demonstrated for the first time in Israel's victory in 2000-2005 over Palestinian suicide bombers during the intifada. See Lior Tabansky, *The Anti-Terrorism Struggle in the Information Age: Palestinian Suicide Bombers and the Implementation of High Technologies in Israel's Response, 2000-2005*, position paper published by Tel Aviv University, May 2007.

11 The great resemblance between the American and Israeli definitions is a result of shared values and a similar scientific and economic level. China, Russia, India, France, and other countries define cyberspace and cyber threats differently. Such a comparison, however, falls outside the bounds of this study.

12 See the discussion above of Karl Popper's theory.

13 A discussion of the status of knowledge appears in Karl Popper, and was mentioned in the preceding section.

14 For a discussion of cyberspace in the context of national security, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2010): 75-92.

15 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).

16 Today, the infrastructure of the computer world is electronics. Before electronics, there were mechanical calculators. And in the future? The practicality of utilizing biological infrastructure for computational purposes has already been demonstrated. DNA computing uses molecular biology and DNA instead of electronic components. Another possibility is peptide computing: bio-molecular computing based on amino acid compounds.

17 Compare the definitions of the US Defense Department, "Joint Publication Jp 3-13: Joint Doctrine for Information Operations," edited by United States Department of Defense, Washington, DC, 2006, with those of the European Union as defined in the tender of the European Defence Agency Study, "Computer Network Operations (CNO) for EU-led Military Operations," 10-CAP-OP-37 (EU Milops CNO Capability) – Annex, August 16, 2010.

18 This includes computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA). The technical basis for the three types of action is identical.

19 See table 2 above.

20 For example, see Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, National Defense University Press: Potomac Books, 2009);

William Lynn III, “Defending a New Domain,” *Foreign Affairs* 89, no. 5 (September-October 2010); Martin Coward, “Network-Centric Violence, Critical Infrastructure and the Urbanization of Security,” *Security Dialogue* 40, no. 4-5 (2009): 4-5; Walter Gary Sharp, “The Past, Present, and Future of Cybersecurity,” *Journal of National Security Law and Policy* 4, no. 1 (2010).

[21] For a discussion of the technical issues, see Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (O’Reilly Media, 2009); and Rick Lehtinen, Deborah Russell, and G. T. Gangemi, *Computer Security Basics* (Sebastopol, CA: O’Reilly & Associates, 2006).

[22] Faulty hardware implanted by the CIA in a system for transporting gas purchased by the Soviet Union allegedly caused an enormous explosion in Siberia in 1982. See W. K. Clark and P. L. Levin, “Securing the Information Highway: How to Enhance the United States’ Electronic Defenses,” *Foreign Affairs* 88, no. 6 (2009).

[23] For the economic consequences, see the discussion by Paul Romer mentioned above.

[24] Following the September 11, 2001 terrorist attacks, the policy support threshold was lowered: sometimes circumstantial evidence, such as ideological support of an enemy or provision of logistic services to terrorists, is sufficient.

[25] A detailed discussion of these matters is beyond the scope of this study.

[26] “The Aurora Experiment,” conducted in the national laboratories in Idaho, US; See James Andrew Lewis, “Thresholds for Cyberwar,” Washington, DC: Center for Strategic and International Studies, 2010.

[27] “The Meaning of Stuxnet,” note 1.

[28] United States, President’s Commission on Critical Infrastructure Protection, “Critical Foundations: Protecting America’s Infrastructures: The Report of the President’s Commission on Critical Infrastructure Protection,” Washington, DC: US GPO, 1997.

[29] See Lior Tabansky, “Critical Infrastructure Protection against Cyber Threats,” *Military and Strategic Affairs* 3, no. 2 (2011): 61-78; Myriam Dunn, “Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory,” in Johan Eriksson and Giampiero Giacomello, eds., *International Relations and Security in the Digital Age* (Routledge, 2007).

[30] Lynn, “Defending a New Domain.”

[31] Israeli governments behaved in this manner for years, when thousands of rockets “trickled” into Israel from Gaza and hit open areas in the western Negev.

[32] One of the measures of software complexity is the number of source lines of code (SLOC). *Windows NT 3.1*, the Microsoft operating system, which was introduced in 1993, had 4.5 million SLOC. *Windows XP*, introduced in 2001, had 45 million SLOC. Linux Fedora 9 has 204 million SLOC.

[33] See Tabansky, “The Struggle against Terrorism in the Information Age.”

34 Ibid., and Lynn, "Defending a New Domain."

35 The dominant encryption method is based on a mathematical principle that it is difficult to factor a number whose factors are prime numbers. Quantum computing has features that will completely eliminate the advantage of the existing encoding methods. When a quantum computer is built, the security field will undergo an upheaval caused by the foundations of encryption being made obsolete.

36 Libicki, *Cyberdeterrence and Cyberwar*. See also Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (2011): 49-62.

Cyber Warfare and Deterrence: Trends and Challenges in Research

Amir Lupovici

In recent years a growing number of researchers have expanded the discussion of deterrence strategy to a host of new threats. Unlike the Cold War era in which the study of deterrence focused primarily on deterrence among nations and superpowers and on nuclear deterrence, recent years – particularly since 9/11 – have seen much research on deterrence strategy in relation to other threats, such as terrorism, rogue states, and ethnic conflicts. These studies share several elements: they are based primarily on an effort to examine the relevance of conditions necessary for successful deterrence, formulated in the context of the Cold War, and to a large degree are policy oriented, particularly regarding the challenges confronting the United States.[1] These same elements dominate the evolving debate on the connection between deterrence and cyber warfare.[2] Much of the research on deterrence strategy and cyber warfare is based on an American perspective. It examines the possibility of successfully implementing the strategy of deterrence in order to prevent cyber attacks, or analyzes the way the US can use cyber warfare in order to deter other threats it faces.[3]

These studies make it clear that the possibility of successful deterrence against cyber attacks is limited with regard to each of the dimensions required for its success: the existence of capability (weapons), the credibility of the threat, and the ability to convey the threatening message to the potential challenger.[4] Nonetheless, there are several elements to consider that under certain circumstances are likely to serve as the basis for successful deterrence even in the realm of cyberspace. This essay surveys the literature and proposes directions for continued research on the topic.

Dr. Amir Lupovici is a lecturer in the Department of Political Science at Tel Aviv University.

This article was first published in *Military and Strategic Affairs* 3, no. 3 (2011): 49-62.

The essay begins by presenting the necessary conditions for a successful strategy of deterrence. It then reviews the central claims regarding the difficulties in applying successful deterrence in cyber warfare vis-à-vis each of these conditions. The third part discusses some benefits and shortcomings of certain factors that may strengthen deterrence against cyber warfare. Finally, it highlights the importance of continuing the discussion of deterrence and cyber warfare, indicating a number of directions for future research.

The Conditions for Successful Deterrence

There are different ways in which actors can try to prevent their enemies from taking undesirable action. The strategy of deterrence by punishment is one of the most studied. This type of deterrence has several definitions,[5] with the definition by George and Smoke, whereby deterrence is the ability to persuade a potential enemy that the price it will pay as the result of carrying out the undesirable action will outweigh any possible profit, is among the most commonly used.[6] This type of deterrence differs from deterrence by denial,[7] which is based on the attempt to persuade potential aggressors that they must avoid taking action because they will fail to attain their goals.[8] The concept of deterrence also differs from the concept of compellence, which is based on the use of threats in order to make an enemy undertake an action, whereas the aim of deterrence is to make the enemy avoid taking undesirable action.[9]

A central question regarding the strategy of deterrence by punishment concerns the conditions under which it is likely to be successful, i.e., cause a potential enemy to avoid challenging the defender. The research, developed mostly during the Cold War and dealing with deterrence between the superpowers, focuses on three central conditions: the defender's capabilities, the credibility of the threat, and relaying the threat message to the challenger.

The first essential condition for successful deterrence by punishment is that the defender be able to exact a price from the challenger. It is therefore not surprising that studies in deterrence arose in particular during the nuclear era, as this weapon allowed both sides to make the cost of a future war very clear. Nuclear weapons gave leaders a crystal ball of sorts, allowing them to see the effects of the next big war and thus encourage them to exert caution in their conduct.[10] At the same time, capabilities are not limited to the non-conventional, as conventional means too may be used to take a toll on the challenger.[11] Moreover, an important part of the capabilities dimension is the means of delivery available to the defender, such as aircraft, missiles, and even roads and vehicles that may play a role in the element of capabilities within the context of deterrence.

A second condition for successful deterrence is the credibility of the threat. In order for the deterrence threat to be effective, the defender must be ready to use the capabilities at its disposal. Various researchers have presented a range of factors that may limit this willingness, e.g., internal or international public opinion, or even the deterrence capabilities of the enemy (the challenger).[12] Common to all these elements is that each in its own way raises the cost of taking action, thereby reducing the actor's credibility in terms of carrying out the threat, if necessary.[13]

The third condition is effective delivery of the messages to the challenger concerning the two previous conditions – capabilities and intentions. In other words, the challenger must be aware of the defender's capabilities and its willingness to use them. Researchers who have developed psychological approaches to deterrence claim that this condition is the most important of all, whereby the perceptions and misperceptions of decision makers directly affect the success of deterrence.[14] In this sense, what matters are neither the capabilities nor the intentions of the defender, rather how they are perceived by the potential challenger.

Finally, because the strategy of deterrence may prevent different types of threats, it is difficult to discuss the conditions for successful deterrence uniformly, as they must be adapted not only to the challenger but also to the type of action the defender is trying to prevent. So, for example, while nuclear weapons may be effective in deterrence against an all-out attack ("general deterrence"), its effectiveness would be lower against more limited types of threats.[15]

Difficulties of Deterrence in Cyber Warfare

Many of the studies analyzing the strategy of deterrence against cyber warfare are based on Cold War theories. Researchers analyzed the central conditions for successful deterrence discussed in the literature: defensive capabilities, the credibility of the threat, and communication, or the ability to transmit the message of capabilities and the credibility of the threat to the challenger. Most researchers believe that an analysis of these conditions shows that the strategy of deterrence may be expected to fail when applied to threats created by cyber warfare.[16]

Capabilities

Cyber warfare allows weak players to move the confrontation into a sphere in which they can maximize profits while risking little – which makes deterrence harder to establish. In effect, an actor that is more technologically developed is also more susceptible to cyber warfare.[17] In fact, the possibility of retaliation against a weaker player is reduced, and thus the ability to establish a credible threat of deterrence is also lessened. For example, it is very difficult to deter players, especially individuals, who do not own information systems that can be threatened with damage.[18] This challenge also exists in the confrontation with nations with less developed information systems infrastructures, where the possibility of creating an effective threat by means of cyber warfare alone is limited.

Credibility

A second challenge to deterrence against cyber threats relates to the defender's credibility. The defender's vulnerability may limit its willingness to tap its capabilities out of concern that retaliation could lead to escalation. The problem for the defender is that such escalation is liable to be much more dangerous to itself than to the challenger, which in turn is likely to strengthen the challenger's belief that the defender's willingness to act is low.[19] This challenge is further amplified by the fact that cyber warfare entry costs are usually lower for the weaker side.[20] In other words, the cost to the challenger of engaging in cyber warfare is often limited, which further increases the difficulties in presenting and executing the deterrent threat required in order to prevent such action.

Internal as well as international public opinion may limit the credibility of the threat of retaliation because of the nature of cyber warfare. In situations in which it is difficult to establish the identity of the source of the attack,[21] the ability to employ a retaliatory measure likely to cause damage is constrained.[22] A potential challenger may view these constraints as undermining deterrence credibility. In this way a potential aggressor, assessing that the chances of the defender making good on its threats are low because of the damage it is likely to incur as a result, will be more willing to take risks and challenge the defender.

Conveying the Threat

A third problem stems from the defender's difficulty in conveying the message about its capabilities and about the credibility of its response to the challenger. Beyond the fundamental problems regarding each of the dimensions described above, challengers may be not only anonymous but even individuals who often have no identifiable physical address.[23] Libicki, for example, claims that to this day the source of the 2007 attack on the Estonian servers is in question: it is not at all certain that the attack was directed from above by the Russian government, as claimed by many who have analyzed the case.[24] The source of an attack can be another state entity, organizations or individuals operating from within the borders of another state, or organizations or individuals operating from within the targeted state. This situation reflects the frequent blurring between crime, terrorism, and warfare.

Moreover, when speaking of deterrence, it is necessary to identify the challenger in advance, before any challenge takes place, in order to target the deterrent threat. This is a key issue, because deterrence is based on the fact that the potential challenger is aware of the defender's capabilities and its willingness to use them ahead of time. However, if the defender is hard pressed to identify the source of the damage even after the attack, it will certainly find it difficult to do so prior to it. While intelligence capabilities may provide a partial solution, the threat that the defender can envision in most situations is general only, and is meant to cover a relatively broad range of potential challengers that the defender thinks would be likely to attack. However, deterrence is more effective when the threat – even if not completely explicit – is aimed at specific actors rather than at anonymous and undifferentiated sets of actors or types of actors liable to issue a challenge.[25]

Another difficulty directly related to the transmission of messages to the challenger involves the specific platform used.[26] This difficulty is amplified in light of the multiplicity of actors capable of creating threats. Unlike the Cold War era, when enemies were a limited number of known state entities with relatively clear capabilities, the number of possible aggressors has multiplied in the information age, lowering the possibility of presenting stable and credible deterrence.[27] The large number and variety of threats possible in cyber warfare creates an arena in which it is more complex to operate and in which it is not completely clear how or to whom to transmit the deterrent message.

Opportunities for Deterrence in Cyber Warfare

Despite these difficulties, the possibility of successful deterrence in cyber warfare exists, at least in part and under specific circumstances. For example, a number of researchers have stressed that retaliation need not be limited to cyberspace but may be effected by more traditional means. Thus, in the case of a state threatening to act by means of cyber warfare, the deterrent threat towards it may be based on the broadest range of capabilities the defending nation has at its disposal. Different threats, whether economic or military, may be effective in deterring a state enemy using cyber warfare against another state entity. Similarly, against threats posed by individuals or terrorist organizations seeking to use cyber warfare, states may, as proposed by a number of researchers (and also several decision makers), choose means of deterrence that do not require use of cyber capabilities. For example, they can employ threats through the judicial system (internal or international) and through internal security services, as well as use of traditional military threats.[28] As such, if actors assess that they will profit by diverting the confrontation into cyberspace, where they enjoy superiority, the actors under attack that might be attacked are under no obligation to limit the theater to cyberspace and may instead move the confrontation into theaters more convenient to them.

Another measure is deterrence by denial. The benefit inherent in this sort of strategy is that it may be based on defensive measures and thus not only be a means of preventing the enemy from acting but also providing a solution in case the challenger decides to act. Moreover, according to Morgan, making extensive use of various defensive measures may help identify the aggressor and strengthen the ability to take retaliatory action, which in turn strengthens deterrence by punishment.[29] Nonetheless, the challenges of using this strategy lie in overcoming problems similar to those linked to the successful use of deterrence by punishment. In both cases, the low entry cost required of challengers when they engage in cyber warfare remains a central difficulty.

Morgan also suggests that serial deterrence[30] may be useful in confronting cyber warfare threats: "Cyber attacks are very likely to turn out to be manageable primarily through applications of serial deterrence, repeated harmful responses over an extended period, to induce either temporary or eventually permanent suspensions of the most bothersome attacks or of attacks by the most obnoxious opponents."[31] While this is an original way to confront threats in cyberspace and represents an interesting attempt to use existing concepts in an innovative way, it is not without difficulty. For example, it is unclear whether the enemy can be affected over time by repeated attempts, as these are liable to teach the challenger that the deterrence of the defender is not working (and that therefore the defender needs to engage in the same repetitive actions).[32]

Another problem regarding a strategy based on serial deterrence is exposing the capabilities of the defender. Although this problem is inherent in every form of deterrence in cyberspace (deterrence by punishment or denial), it is particularly acute when what is at issue is deterrence over time, as with the strategy of serial deterrence.[33] In such situations, exposing the offensive capabilities as the consequence of repeated attacks may serve as the basis for knowledge or inspiration for the challenger.[34] Morgan himself has referred to this issue and argues that revealing capabilities is liable not only to provide inspiration to enemies and motivation to attain similar capabilities but is also likely to allow enemies to prepare for a future threat, thereby damaging its measure of effectiveness.[35]

Directions for Further Research

While indeed some scholars have started to suggest new directions for research on deterrence in cyberspace, I would like to point to two main avenues through which cyber deterrence thinking can be further developed. First, research dealing with threats in cyberspace should be sharpened. It seems that there is a growing gap between practice and types of threats in the international arena, and the way in which research in this field examines the strategy of deterrence. This gap exists in other research dealing with deterrence, but it is particularly prominent in the realm of cyberspace, which includes many types of interaction between many different sorts of actors representing various kinds of threats. Therefore it is necessary to expand the discussion about the types of actors, the threats they create, and the ways and challenges of deterring each one. In addition, similar to the broader research relating to the strategy of deterrence, there is a tendency to focus on the deterrence of states against various types of players (e.g., terrorist organizations, rogue states),[36] while an important aspect not given sufficient attention is the deterrence of these actors against the states they seek to challenge. This aspect exists also in cyber warfare and intensifies the problems of states that must now deal with a much more complex setting than in the past.

Moreover, research on cyber warfare tends to deal with more classical aspects of security, whereas the arena of threats is complex and varied.[37] For example, states are worried about the growing strength of economic players (such as Google) or ideological ones (e.g., individuals seeking to promote government reforms) using cyberspace. Irrespective of whether or not the existing definitions of cyber warfare include interactions with these actors, a considerable contribution could be made by analyzing these relations using theories of deterrence. The concept of the strategy of deterrence might be used, for instance, to study the interactions between Google and China with regard to the implied or direct threats presented by these players to one another in the context of search engine censorship. In this sense, dividing research on deterrence and cyber warfare according to different types of threats (e.g., internet war, cyber terror, cybercrime, cyberwar) and the actors operating them (states, individuals, economic institutions) may be not only more accurate and productive but may also identify the conditions for raising the chances of success of each actor's strategy of deterrence against its enemy.

The second theme that should be expanded is analysis of the traditional literature on the strategy of deterrence in critical and original ways. This has already been done in some of the essays published on the topic. However, it remains to analyze further concepts regarding deterrence strategy already discussed in the literature, such as immediate deterrence,[38] general deterrence, and extended deterrence,[39] and to try to understand the significance and relevance of applying these practices to cyberspace.

Similarly, the concept of ambiguity should be studied. This concept may serve as a framework for practical thinking in confronting the dilemma inherent in the need for revealing capabilities on the one hand,[40] balanced against the concern that the enemy will be able to exploit this exposure to increase its own strength and immunity to attack. Using insights developed in different contexts may provide an interesting foundation for developing ideas on cyberspace ambiguity, not only with regard to intention and willingness to make good on threats but generally with regard to the existence of capabilities. In this respect, it is possible, for example, to analyze the different efforts made by several nations in recent years in the field of cyber warfare. Not only are the means developed by nations likely to strengthen their strategy of deterrence against these threats, but the very prominence of these efforts may also serve as a deterrent tool. The same is true of the American establishment of a strategic command to manage cyber warfare:[41] it has a range of objectives and functions, but its very reference and prominence allow not just improvements in capabilities but also demonstrate US willingness to invest resources in reducing threats and damage. It may be that stressing the desire to invest in measures of this sort and revealing the scope of the budgets, resources, and manpower dedicated to the subject – even absent a detailed breakdown of the measures acquired and their capabilities – can help increase the credibility of the deterrent message against threats in cyberspace, especially with regard to threats involving high levels of violence on the part of other nations. In other words, a partial revelation of capabilities while maintaining ambiguity about their essence allows for a reduction of the harmful effects described above but also transmits a forceful message. At the same time, one may expect that the low entry threshold for operating in cyberspace, especially in cases of asymmetrical confrontations, will continue to present a challenge to establishment of a strategy of deterrence seeking to prevent threats in this realm.

Conclusion

The research that deals with cyber warfare deterrence discusses primarily the difficulties inherent in deterring enemies from using this strategy. Although deterrence may work under certain circumstances, the problems associated with the defender's capabilities, the defender's willingness to use them, and the defender's ability to convey a message of deterrence to its potential enemy greatly limit the possibility of successful deterrence. Nonetheless, in light of the benefits inherent in the strategy of deterrence in reducing the scope of violence of conflicts, it is important to try to further the research dealing with the connections between deterrence and cyber warfare. This essay has indicated some directions for further thought and development of these ideas. However, as claimed by Morgan, these insights should be applied carefully, because additional empirical knowledge about the essence of cyber warfare is required, in terms of both the damage it can generate and the way in which it may be used.

Notes

[1] Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda," *International Studies Quarterly* 54, no. 1 (2010): 705-32.

[2] "Cyber warfare" refers here to a certain type of information warfare, though at times the concept of "information warfare" serves as a synonym for cyber warfare. This type of warfare is based on various attempts to prevent, disrupt, or destroy the enemy's information systems, while protecting the information systems of the defender against similar threats. See Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996): 93-107; Gary F. Wheatley and Richard E. Hayes, Infor*mation Warfare and Deterrence* (Washington, DC: National Defense University Press, 1996), pp. v-vi, 5-6; Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," *Parameters* 26, no. 3 (1996): 83, 86-90. For a review of central concepts in cyber warfare, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92.

[3] On the general tendency of research dealing with cyber warfare and security to analyze policy oriented issues and to minimize the incorporation of broader theoretical dimensions, see Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27, no. 3 (2006): 221-44.

[4] This essays use the common terms to describe the actors involved in deterrence strategy: the *defender* – the actor seeking to use the strategy of deterrence in order to prevent undesirable action against it, and the *challenger* – the actor seeking to act against the defender. The sometime usage of the alternative terms – the deterring actor or the deterred actor – is problematic because it assumes the success of the strategy.

[5] For an excellent survey of definitions of the concept of deterrence by punishment, see Patrick M. Morgan, *Deterrence Now* (New York: Cambridge University Press, 2003), pp. 1-2.

[6] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), p. 11.

[7] Deterrence by denial also differs from the strategy of defense. While there is an overlap, defense seeks to provide a solution to a situation in which the strategy of deterrence has failed, while deterrence by denial seeks to prevent the action by making the challenger understand that it lacks the capacity to execute the action because of the defender's capabilities.

[8] Glenn Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961). Nevertheless, deterrence by punishment and deterrence by denial may in theory support one another. If a potential challenger is made to realize that not only are its chances for success low but it will also be

required to pay a steep price for aggression, there is a higher chance it will refrain from action.

9 Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

10 Albert Carnesale, Paul Doty, Stanley Hoffmann, Samuel P. Huntington, Joseph S. Nye, Jr., and Scott D. Sagan, *Living with Nuclear Weapons* (Cambridge: Harvard University Press, 1983).

11 For a discussion of conventional deterrence, see., e.g., John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983) and Jonathan Shimshoni, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca: Cornell University Press, 1988).

12 For example, it has been claimed that the development of international norms calling for the ban on nuclear weapons and international public opinion in support of this call have weakened the strategy of deterrence because they have raised the cost of their use of them. See T. V. Paul, "Nuclear Taboo and War Initiation in Regional Conflicts," *Journal of Conflict Resolution* 39, no. 4 (1995): 696-717.

13 Various researchers have debated the question of how to increase the credibility of the threat and have even proposed measures to attain this goal, e.g., by means of costly signals. See James Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (1994): 577–92. Still, some researchers have cast doubt on the effectiveness of some of these measures. For a discussion of the topic, see, for example, Paul Huth, "Reputations and Deterrence: A Theoretical and Empirical Assessment," *Security Studies* 7, no. 1 (1997): 72-99.

14 Morgan, *Deterrence Now*, pp. 15-16.

15 For an excellent survey demonstrating the different types of Israeli deterrence, see Uri Bar-Joseph, "Variations on a Theme: The Conceptualization of Deterrence in Israeli Strategic Thinking," *Security Studies* 7, no. 3 (1998): 12-29.

16 Harknett, "Information Warfare and Deterrence"; Br*uce* D. Berkowitz, "Warfare in the Information Age," in John Arquilla and David F. Ronfeldt, eds., *Athena's Camp: Preparing for Conflict in the Information Ag*e (Santa Monica: RAND, 1997), pp. 183-84; Emily O. Goldman, "Introduction: Security in the Information Technology Age," in Emily O. Goldman, ed., *National Security in the Information Age* (London: Taylor & Francis, 2004), p. 3; John Arquilla. "Thinking about New Security Paradigms," in Emily O. Goldman, ed., *National Security in the Information Age* (New York: Routledge, 2004), pp. 210-13. Morgan reaches similar conclusions, claiming that the different elements affecting the practices of deterrence of the Cold War, based both on this strategy and on supportive measures such as arms control, are less relevant to deterrence in cyberspace, though he does not entirely rule out the possibility of using different types of deterrent strategies in confronting these threats. See Patrick M. Morgan, "Applicability

of Traditional Deterrence Concepts and Theory to the Cyber Realm," in John D. Steinbruner et al., eds., *Proceedings of a Workshop on Deterring Cyberspace* (Washington: National Academies Press, 2010), pp. 55-76. In light of the various limitations regarding the ability to establish deterrence against cyber warfare, it has been proposed – especially for the United States, which is the primary subject of the research – to take alternative measures, such as using defensive means. See Wheatley and Hayes, Infor*mation Warfare and Deterrence*, p. 9, and James Adams, "Virtual Defense," *Foreign Affairs* 80 (2001): 107-12.

17 Harknett, "Information Warfare and Deterrence"; Wheatley and Hayes, *Information Warfare and Deterrence*, p. 9; Berkowitz, "Warfare in the Information Age," pp. 183-84; Martin C. Libicki, *Conquest in Cyberspace* (Cambridge, Cambridge University Press, 2007), p. 272. On societies' vulnerability to electronic attacks, see Ron Deibert, "Circuits of Power: Security in the Internet Environment," in J. P. Singh and James N. Rosenau, eds., *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (NY: SUNY Press, 2002), p. 115. For sensitivity to threats – both external and internal – to information systems, see Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND, 2009), www.rand.org/pubs/monographs/2009/RAND_MG877.pdf. At the same time, for Libicki the scope of threat created by cyber warfare in the present age is neither clear nor certain. According to Libicki, the issue of the scope of damage liable to be created by cyber warfare is a central question at the heart of the debate about the importance of the strategy of deterrence against this type of warfare (*Cyber Deterrence and Cyberwar*, p. 36). For similar reasons having to do with the paucity of available information and the newness of the subject, Morgan cautions against drawing hasty conclusions about the possibilities of deterrence against cyberspace threats, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," pp. 61-62.

18 Libicki, *Cyber Deterrence and Cyberwar*, p. 26.

19 Harknett, "Information Warfare and Deterrence," p. 104.

20 Molander, Riddile, and Wilson, "Strategic Information Warfare," p. 87.

21 For more on the difficulties in identifying the source of cyber warfare attacks, see also Libicki, *Cyber Deterrence and Cyberwar*, pp. 44-45.

22 For more on internal and international public opinion limiting the possibility of using force, thereby affecting the defender's deterrence, see., e.g., Robert Jervis, "Deterrence, Rogue States, and the Bush Administration," in T. V. Paul, Patrick Morgan, and James Wirtz, eds., *Complex Deterrence*: *Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), p. 153.

23 Wheatley and Hayes, Infor*mation Warfare and Deterrence*, p. 9; Harknett, "Information Warfare and Deterrence," p. 104; Berkowitz, "Warfare in the Information Age," pp. 183-84; Anthony Cordesman and Justin Cordesman, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection:*

Defending the US Homeland (Westport: Praeger, 2001), p. 7; and Arquilla, "Thinking about New Security Paradigms," pp. 210-11.

[24] Libicki, *Cyber Deterrence and Cyberwar*, pp. 1-3.

[25] The reason is that a deterring threat must be adapted to the type of threat and the type of element posing it. Therefore it is important to establish the deterrence in the context of the threat for the specific aggressor. For example, deterrence against a state actor enjoying sovereignty in a particular territory and possessing valuable target differs from a non-state actor and therefore requires the presentation of different types of threats. This issue has in recent years been at the center of an extensive debate in the context of tailored deterrence, particularly in the context of deterring terrorism. For a discussion of the concept, see Jeffrey S. Lantis, "Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice," *Contemporary Security Policy* 30, no. 3 (2009): 469-71. For a discussion of the concept vis-à-vis cyber warfare, see Richard L. Kugler, "Deterrence of Cyber Attacks," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), pp. 331-33, and Lantis, pp. 469-71.

[26] Harknett, "Information Warfare and Deterrence," pp. 98-100.

[27] Libicki, *Conquest in Cyberspace*, p. 272. For more on the effect of the Revolution in Military Affairs on deterrence and the ability to deter, see Morgan, *Deterrence Now*, pp. 219-24.

[28] Hayes and Wheatley, Infor*mation Warfare and Deterrence*, pp. 13, 19-20; Kugler, "Deterrence of Cyber Attacks," p. 328; and in Cordesman and Cordesman, *Cyberthreats, Information Warfare, and Critical Infrastructure Protection* , p. 7.

[29] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 59.

[30] Doron Almog uses the similar concept of "cumulative deterrence" with regard to the way to deter terrorist threats not in the cyber arena. See Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4 (2004-2005): 4-19.

[31] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 59.

[32] Lupovici, "The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda," p. 722.

[33] Thus, for example, a challenger is likely to learn about the defensive measures (or be inspired to attain such measures) on the basis of the means used by the actor trying to use deterrence by denial, thereby limiting the ability to deter effectively with this strategy.

[34] Similar criticism was raised after the reports about the Stuxnet virus, which reportedly disrupted the systems of the Iranian reactor in Bushehr. The concern presented by a number of information security specialists was that this cyber attack would serve as inspiration not only for what can be

done using such warfare but also that some of the codes of the virus itself were revealed and could conceivably serve various actors in their attempts to damage sensitive infrastructures. See., e.g., "Experts Fear Hackers Can Launch Stuxnet-Like Attacks on Power Plants, Prison Gates," *The Globe and Mail,* October 24, 2011.

35 Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," p. 63.

36 For reference to this issue in the context of information warfare, see, e.g., Goldman, "Introduction: Security in the Information Technology Age," p. 3.

37 For a discussion of the range of these threats, see Tabansky, "Basic Concepts in Cyber Warfare," especially pp. 80, 86-88.

38 A basic distinction existing in the study of deterrence deals with the difference between general deterrence, based on the attempt to prevent the enemy from thinking at all about the possibility of attacking (e.g., as with nuclear deterrence), and immediate deterrence, touching on a situation in which an actor would like to take an action (e.g., move troops) and by using threats the defender dissuades the enemy from taking such action. An important discussion in this context could deal with the meaning of each of these types of deterrence in cyberspace.

39 Libicki, for example, has started to analyze extended deterrence in cyberspace. See Libicki, *Cyber Deterrence and Cyberwar*, pp. 104-6), and it is possible to develop the discussion of theoretical issues discussed in the literature with regard to extended deterrence. For a discussion of the concept of extended deterrence see., e.g., Paul Huth,, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988).

40 The literature about deterrence stresses that it is necessary to transmit the threat message to the enemy, including the price it will have to pay. Therefore messages about defensive capabilities or revealing capabilities have been noted as important elements in this context.

41 "U.S. Cyber Command Fact Sheet," *US Department of Defense*, May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

In Defense of Stuxnet

James A. Lewis

Revelations about Stuxnet and Flame have provoked a chorus of dire warnings on the dangers of cyber warfare and the need for action. Yet the most troubling question to emerge from these revelations is why, if cyber warfare is such a critical issue, are so many people so badly informed about it? Suggestions that Stuxnet or Flame have increased risk are based on a faulty understanding of how much risk already exists in cyberspace, the already high frequency of state-sponsored malicious cyber action,[1] and the rapid growth in many countries' military capabilities. It is, rather, more accurate to see Stuxnet and Flame as episodes in the ongoing contests between the US, Iran, and Russia.

The belief that Stuxnet increases risk to the US or its allies is based on a number of erroneous assumptions. Notions of blowback, collateral damage, or opening a Pandora's Box do not make sense in the context of how cyber attack techniques have been used and have evolved over the last three decades. Stuxnet did not reveal a new military capability that others will be quick to copy. Cyber attack is a recognized military and intelligence capability that has been in use for years. Perhaps forty states are acquiring or have already acquired military cyber capabilities,[2] including the ability to launch cyber attacks. Most of these national programs are shrouded in secrecy, and there is disagreement on how existing international law that governs armed conflict should apply to the new mode of attack. However, every advanced military already has a cyber attack capability and many other nations wish to acquire it.

The allegation about the US role in Stuxnet was not much of a surprise; most nations had already concluded that the US was responsible, and they were not astonished to see software become a tool of coercion and attack.

Dr. James A. Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS).

This article was first published in *Military and Strategic Affairs* 4, no. 3 (2012): 65-76.

The use of cyber techniques as intelligence tools dates back to the 1980s; cyber attack by militaries dates back to the 1990s.[3] The development of offensive cyber techniques has accelerated in this century, when high speed global networks became widely available and the internet moved from being an accessory to being the central infrastructure for economic and governmental activity. Whether it is "network-centric" warfare or "warfare in informatized conditions" (as China puts it), cyber attack is not new to military planners.

From Espionage to Attack

Although Stuxnet and Flame have been hailed as the dawn of cyber war, this is mistaken on several counts. Cyber attack is not new, and while sabotage may involve the use of force, not all acts of sabotage count as an act of war. Calling Stuxnet and Flame cyber war perpetuates the exaggeration and imprecise reasoning by analogy that has dogged inquiry into cyber security from the start. Cyber "attack" offers new tools for coercion, espionage, and attack rather than an unprecedented and unique category of conflict.

The line between espionage and attack in cyberspace is very thin. The network penetration and control necessary for espionage could be used to disrupt critical services. An opponent who can gain controlling access to a network can also disrupt and perhaps destroy. One way to think of cyber attack is as the "weaponization" of signals intelligence, transforming the passive collection of information into active disruption. This means, to put "cyber disarmament" in context, that to ban cyber attack we would also need to ban espionage, an activity that no nation will agree to abandon.

Flame was one of the many intelligence collection programs that are found on the internet. There is public knowledge of a dozen programs like Flame used for cyber espionage. Technology has changed how nations spy on each other and cyber espionage has become a central element of national collection programs. The internet has created what some intelligence officials call a "golden age" for espionage.

This golden age is entering its third decade. In the early 1980s, Russian intelligence services used West German hackers to penetrate US military and research networks and exfiltrate information. Chinese security services have waged a long and successful campaign against the networks of the US and its allies, and have engaged in massive state-sponsored industrial espionage. If Stuxnet pointed towards the US and Israel as the nations with the most to gain from disrupting Iran's nuclear effort, what nation would gain the most from spending immense resources to track Tibetan human rights activists? In the last fifteen years, many collection programs like Flame have become public; presumably there are others that are better hidden. For espionage, cyber techniques are in good measure an extension of traditional signals intelligence capabilities, and for China, an extension of the distributed approach using multiple civilian agents seen in Chinese human collection programs.

Both China and Russia use cyber exploits in ways that differ from the cyber activities of Western services in important and potentially destabilizing ways. Both rely on proxies – private hackers acting at the direction of the state for government purposes. Proxies provide an increasingly feeble degree of deniability – does any serious observer believe that China and Russia do not control what happens on their networks – and an advance line of attackers that can shield state actions and, if necessary, be sacrificed to placate other nations. Russian proxies have focused on financial crimes, Chinese proxies on industrial espionage. Both nations provide a degree of training and support to their proxies and insist on one cardinal rule – no hacking against domestic targets. If this rule is observed and if the proxies cooperate in tasks assigned by the state, they are free to act against targets in other nations. Russian proxies were responsible for the exploits against Estonia and Georgia (the latter were precisely coordinated with Russian military plans);[4] Chinese proxies were responsible for the exfiltration of data from many economic and military targets in the US and other nations.

In contrast, neither the US nor its allies use proxies to engage in state sponsored financial crime, and the US does not engage in industrial espionage. US doctrine for the use of cyber techniques as an extension of traditional tools of coercion is different, but certainly not unprecedented.

Cyber Attack and the Weaponization of Signals Intelligence

Capabilities like those contained in Stuxnet reflect years of development and experimentation in how to exploit digital networks to gain military power. Stuxnet had advanced destructive capabilities, as it was designed to affect industrial control systems – specialized computers that run machinery – but it was an extension and refinement of existing software attack techniques. The ability to use software to disrupt industrial control systems and cause physical destruction was demonstrated in a 2005 experiment at Idaho

National Labs. Perhaps five nations have this capability – the US, the UK, Israel, Russia, and China - and many other nations are trying to acquire it. In this regard, the US may be *primus inter pares*, but it has peers (or near peers) when it comes to cyber attack. Stuxnet may be the most advanced such "weapon" (another hallmark of the US), but it is by no means a unique capability.

Cyber attack is another option for military planners. With Stuxnet, for example, planners could weigh the merits and disadvantages of cyber attack, air strike, special operations teams, saboteurs, or missiles. Existing military doctrines have been extended and adapted to the new mode of attack. Nations have created cyber attack capabilities and have developed doctrine and strategies for their use. These national doctrines are not the same in all countries. We are in a period of experimentation as nations evaluate this new military capability and explore how best to use their new cyber capabilities. In addition to Russia's use of cyber "attack" in Estonia and Georgia and alleged Israeli use in Syria, we have seen Russia and China carry out reconnaissance for attacks on US critical infrastructure (according to the head of the US National Security Agency),[5] and probes by Iran against Israel and Gulf states. The US used cyber attacks in the 1990s during the conflict with Serbia and against Iraqi air defenses between Persian Gulf wars.

The US, Russia, China, and others include attacks on critical infrastructure as part of their doctrine for the military use of cyber attack. Publicly available doctrine suggests that each country makes decisions on the use of cyber attack in a manner consistent with planning for the use of other long range weapons – such as the benefits of a strike, the risk of escalation, and the potential for collateral effect. US doctrine shows some parallels to thinking about strategic bombing and the use of aerial bombing to reduce the will and capacity of an opponent to resist while avoiding a prolonged confrontation with its military forces. Russian doctrine pays greater attention to disrupting political stability and military command systems through cyber techniques, and this resembles Soviet doctrine on crippling first strikes against NATO by attacking critical infrastructure. China's doctrine is more opaque, but public discussion has emphasized attacks on infrastructure to disrupt the US ability to intervene in a regional crisis.[6]

Putting cyber attack in the context of military decision making (and assuming that state and non-state actors overall have similar military planning processes) has implications for use of cyber attacks. Nations are no more likely to launch a cyber attack that causes physical damage against the US or its allies after Stuxnet than they were before its discovery, nor are they likely to stop using cyber techniques for espionage and political coercion. We have not seen physically damaging attacks that could cause damage, destruction, or casualties (as opposed to espionage and crime) against the US and its allies from those countries with this capability because they assess the risk of a violent response as too high. This is the same reasoning that keeps them from launching aircraft or missiles against the US. However, international practice and law do not justify the use of force in response to espionage and crime, making the risk of a violent response small and acceptable.

This reluctance to attack may change as other nations with a different tolerance for risk, such as Iran, acquire advanced cyber attack capabilities, or as actors who overestimate their ability to remain covert gain advanced capabilities. What we do not know is how far non-state actors have advanced in their ability to develop similarly destructive techniques. The only indisputable evidence is that to date, we have not seen non-state actors engage in such attacks. This may reflect an absence of motive or of capability, and we cannot estimate how quickly such actors may gain the ability to carry out Stuxnet-like attacks.

To the credit of the designers of Stuxnet, it was carefully written to avoid collateral damage. Other attackers may not be so careful, but this has nothing to do with access to the Stuxnet code. Potential opponents still go through the same calculus of benefit and risk in deciding whether to use force against the US, and they are deterred by the likely US military response using all military assets at its disposal, not just cyber attack. They may now cite Stuxnet as part of any public justification of attack, but this will be an excuse, not part of their decision making. Nations are no more likely to launch a cyber attack against the US or its allies after Stuxnet than they were before its discovery.

How militaries will use the potential of cyber attack has important implications that explain why Stuxnet and Flame did not greatly change matters. Like any weapon, cyber attack has its own characteristics. Cyber attacks can be fast, covert, and contain less political risk in some scenarios. Their drawback is a less destructive payload. An attack planner will consider these aspects, and assess the likelihood of a cyber attack achieving the desired effect at lowest "cost" when compared to other modes of attack. In some scenarios, cyber attack is preferable. The alternatives to Stuxnet included sabotage teams, airs strikes, missile strikes, or even occupation of the territory by conventional forces. Even this short list of potions, all of which pose greater risk of friendly losses, turmoil, and escalation, is enough to indicate why cyber attack was preferable

Nations already routinely use "cyber attacks" in ways that serve their needs. Other nations have the ability to carry out an attack like Stuxnet; but their strategies emphasize other goals, and to date, it has not been in their interest to cause physical damage. Russia and China have demonstrated advanced capabilities and could launch Stuxnet-like attacks should such attacks seem useful to them. That cyber conflict before Stuxnet was largely hidden from public view does not mean it was not taking place.

Another erroneous assumption is that Stuxnet was an event like Hiroshima, unleashing a new and uncontrollably destructive military force. But there is no Oppenheimer to chant of Stuxnet, "'Now I am become Death, the destroyer of worlds."[7] Despite the apparently tempting desire to compare cyber attack to nuclear weapons, this comparison is fallacious. Even small nuclear weapons have immense destructive power. Cyber attacks do not. They are a support weapon, useful to shape the battlefield in advantageous ways, but their effect is neither massively destructive nor fatal, and they do not pose an existential threat to nations. Cyber attack can be best compared to a missile, offering a fast, long range strike, with greater covertness (perhaps) but a smaller destructive payload. This limited destructive capability does not mean we should welcome the disruption of an artificial financial panic or a blackout that could last weeks, but we must also avoid exaggerating the effect of a cyber attack.[8] Stuxnet called attention to the vulnerability of modern software, but the destructive power of cyber attack is nowhere near that of nuclear weapons or even a sustained assault using kinetic weapons.

The Regional Contest

Stuxnet's code is now publicly available and some worry that it could now be reused by others. This ignores one of the primary limitations of cyber attack. They are usually "single-use" exploits. Once the "zero days" and other programming errors in operating systems or industrial control systems are exposed by an attack, they are usually fixed. The publicly available Stuxnet code was part of a larger and more complex exploit that involved a range of espionage techniques. The code was only part of the exploit and by itself insufficient. Stuxnet, if relaunched, would not work. The best evidence of this is that while many systems around the world were infected, only one, in Iran, was damaged.

Iran may seek revenge for Stuxnet, but it was not news to the Iranians that the US and other nations are engaged in covert campaigns aimed at hampering their illicit nuclear weapons program, nor have the Iranians ever been shy about using violence against the US or Israel. Iran is responsible for the deaths of American personnel in Beirut, the Persian Gulf, and Iraq. Stuxnet is another chapter in a covert, sporadic conflict between the US and Iran that has been going on for more then thirty years.

Iran is also not bashful about uttering threats, and makes no secret of its own desire to develop and use cyber attack techniques. Venomous rhetoric against Israel by Iranian leaders may simply be rantings designed for a domestic audience, but this does not excuse them. States bear responsibility for the public remarks of their leaders. Given these threats, and in the context of repeated violations of its international commitments regarding nuclear weapons, to say that a covert action involving the use of software against Iran's nuclear program is inappropriate – an action that produced no casualties or collateral damage – is a strange conclusion.[9]

If we accept that the US was involved in Stuxnet, this is also not a surprise. The US has a history of using covert action against aggressive, non-democratic regimes. The capability was developed in World War II (under the tutelage of the British) and was refined and expanded during the Cold War. But the US has never used covert force against a democratic nation or against a nation that posed no threat to international peace. We can question the US ability to discern threats to peace – there have been many errors, but Iran is not one of them. Covert action is preferable to other military responses in many cases, as it reduces the risk of direct confrontation or expanded conflict. Covert action is a middle ground between acquiescence and open war, another tool for legitimate defense for state use even if it is repugnant to some.

The US justified these interventions on the grounds that it is leading a coalition of nations in defense of democracy – a role thrust upon it by World War II and the Cold War. This role was generally accepted by the community of democracies between 1941 and 1990. Even if we do not accept the assertion that the US still leads a coalition of nations in defense of democracy, we can make a strong case that Iran's behavior threatens US security and international peace, justifying active measures in response.

The advantages of Stuxnet are many and the only regret we should feel is that it was discovered prematurely. Launching Stuxnet posed much less political risk than air strikes. There was no collateral damage, no televised images of smoking buildings and weeping civilians, and no downed pilot being marched through the streets of Tehran en route to being tortured. The "weaponized" code cost much less than a single F-16.

The Missing Political Context

The emphasis on cyberwar in the public discussion of Stuxnet and Flame has meant that interesting questions have gone largely unasked. Seeing an opponent "stumble" across a complex, covert operation, especially if this happens more than once, suggests that we should consider explanations other than coincidence. The hypothesis about both Stuxnet and Flame worth exploring is the connection of the revelations to Russia. The revelations about Flame served a larger Russian political agenda on internet governance and cyber security. Putting Stuxnet and Flame in the context of the practice of espionage and covert political action may better explain what occurred than a focus on warfare.

In particular, the way that information about Flame was released is consistent with an effort at political manipulation to win support at upcoming multilateral meetings on internet governance later this year. Russia and others would like the International Telecommunications Union (ITU) to play a larger role in cyber security and internet governance. A greater role for the ITU would undercut any perceived American "hegemony" in cyberspace and perhaps reduce the risk Russia faces from the untrammeled access to information that the internet can provide. Russia may also seek to "stigmatize" the use of cyber attacks and wing support for a treaty banning weapons like Stuxnet in an effort to undermine an area of perceived US military advantage. This is a standard trick in international negotiations, to propose constraints that erode an opponent's capabilities more than your own (similar to the efforts in the 1980s to manipulate nuclear disarmament in Europe to reduce NATO capabilities more than those of the Warsaw Pact).

There are unusual associations in the entire affair. The Chief Executive Officer of the company that found Flame was an unofficial spokesperson for the Russian government at the 2011 London Cyber Conference. In November 2011, his company and the ITU announced they were forming a partnership to promote global cybersecurity.[10] The company says that it found Flame after the ITU asked it, in an unprecedented request, to look at data breaches in the Middle East, on the basis of which the ITU announced a global warning on cyber security, which was also unprecedented.[11] This could be straightforward; an alternate hypothesis which cannot be rejected is that this is a larger political maneuver designed by the Russians to influence opinion in key nations. It is a common intelligence technique to use a proxy to release damaging information about an opponent and Russia relies heavily on proxies in its own cyber espionage practices. These anomalies are suggestive and point to alternative hypotheses, the most plausible being that Western services created Flame to spy on Iran, and that Russia exploited its discovery for political purposes.

In recent years, Russia and China (sometimes acting through the Shanghai Cooperation Organization) have begun to develop an international strategy that would create an internet more accommodating to their interests. They believe that the information dominance of the West is part of a larger strategy of hegemony rather than a reaction to the failure of state-run media. While they can suppress their own citizens, they cannot suppress foreign sources of information. They have invested heavily in censoring technologies but have also sought international agreement to define information as a weapon that must be controlled. The internet creates political pressures not easily controlled by authoritarian regimes that can be a threat to their regimes (how much of a threat is another matter). This larger effort to restrict access to information and undercut the US is the political context for Flame.

At roughly the same time that Flame and Stuxnet were attracting such attention another piece of spyware went largely unremarked. A popular proxy service (which allows internet users to evade government controls) was compromised so that every person who downloaded the proxy program also downloaded malware that provided their user name and machine name and logged all of their keystrokes. The Simurgh malware affected thousands of people. The researchers at the University of Toronto's Munk School who found it believe it was targeted at Iranian and Syrian dissidents.[12] The malware created far greater risk than Flame but was not as loudly trumpeted, nor did the ITU issue a global warning. One possible explanation for this anomaly is that Flame fit a larger political agenda and Simurgh did not.

The relation of Flame to international negotiations on cyber security (and internet governance) provides important background on the multilateral efforts to make cyberspace more secure. One unremarked aspect in the recent public commentary is that the new risk from cyber attack became part of the international security agenda several years ago, when the military and security risks of high speed global connectivity became apparent. Cyberspace, weakly governed and poorly secured, is a now a source of international instability. Nations fear inadvertent escalation into a larger kinetic conflict more than the actual effect of cyber attack, given its limited potential for damage. A serious dialogue on how to reduce risk has been underway at least since the Russian effort to coerce Estonia using cyber techniques in 2007. The "attacks" against Estonia in 2007 posed much greater danger to international stability than Stuxnet, as it threatened to trigger armed conflict between NATO and Russia.

As a result, there are discussions in many official forums on how to reduce risk and increase stability. These include the UN's Group of Government Experts, the Organization for Stability and Cooperation in Europe, the Asian Regional Forum and the London Conference Process. The Organization of American States has held meetings on cyber security. The US, Russia, and China are engaged in bilateral discussions on cybersecurity, and the US has engaged in similar discussions with close allies. To portray Stuxnet and Flame as a grave new danger is more of a rhetorical device to gain negotiating advantage than a serious analysis of international security.

Conclusion

Technologically advanced militaries have created cyber techniques and will make use of them to advance their interests. There is conflict (even if it is not "warfare"). If Stuxnet and Flame point to any risk, it is that a lack of knowledge of the military and negotiating terrain for cyber security and a quasi-superstitious understanding of cyber attack will impede efforts to make cyberspace more stable and secure. Stuxnet and Flame were not apocalyptic, not particularly new, and not the dawn of some new era of warfare. Technology has reshaped warfare since the start of the industrial age. We may not like this, but states and armed groups have rarely forsaken a new capability. Nations may reject massively horrific weapons, but everything else will be used. Cyber attack is no different. States will behave as they have always behaved, and simply take advantage of new technologies to achieve their purposes.

Notes

[1] Malicious cyber action can be defined as software sent over digital networks to illicitly access target computers and execute instructions without the owner's permission.

[2] James A. Lewis, Katrina Timlin, "Cybersecurity and Cyberwarfare," UNIDIR Resources, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

[3] Clifford Stoll's *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) details Soviet cyber espionage in the 1980s. While there is little public discussion of cyber attacks by the US against Serbia in the 1990s, US officials have provided details in interviews.

[4] US Cyber Consequences Unit, "Overview by the US CCU of the Cyber Campaign against Georgia," August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

[5] "Militarisation of Cyberspace: How the Global Power Struggle Moved Online," *The Guardian*, April 2012, http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle.

[6] See, for example, Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 2009.

[7] Robert Oppenheimer, scientific head of the project to develop an atomic bomb, quoted this statement from the Bhagavad Gita at the first successful test.

[8] "Cyber-like-nuclear" scenarios involve long chains of dubious assumptions about the political effect of attack and the resilience of the target. For a longer discussion, see James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats**,"** CSIS, December 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

[9] See, for example, Robert Wright, "How Obama's Cyberweapons Could Boomerang," *The Atlantic*, June 2012; Misha Glenny, "We will Rue Stuxnet's Cavalier Deployment," *Financial Times*, June 2012, http://www.ft.com/cms/s/0/6b674600-afc7-11e1-a025-00144feabdc0.html#axzz25KCLvt33**;** or Jason Healy, "Stuxnets are not in the US National Interest: An Arsonist Calling for Better Fire Codes," Atlantic Council, June 2012. Note that the triggering event for these cries of anguish was not the actual attack, but a news story about the attack, illustrating the media driven nature of much of the discussion. Noise in the press is not a good measure of actual risk.

[10] "ITU Teams Up with Kaspersky Lab for ITU Telecom World 2012," http://www.kaspersky.com/about/news/business/2012/ITU_Teams_Up_with_Kaspersky_Lab_for_ITU_Telecom_World_2012.

11 "Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat," http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat/.

12 Munk School of Global Affairs, "Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor," May 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2/.

Unraveling the Stuxnet Effect:
Of Much Persistence and Little Change in the Cyber Threats Debate

Myriam Dunn Cavelty

Cyber threats have been on the security political agenda for a number of years. Since RAND researchers John Arquilla and David Ronfeldt suggested in 1993 that "cyberwar is coming!"[1] cyberwar has become the most prominent buzzword in the debate surrounding computers, national security, and cyberspace. Being at the mercy of well-publicized events and occurrences, interest in the topic used to flare up whenever anything involving the aggressive use of computers hit the news, only to disappear again when other issues took over the limelight.

This changed in 2010. In particular, it was Stuxnet, the sophisticated computer worm written to sabotage systems that control and monitor industrial processes, that stirred up the international community in major ways and catapulted the cyber topic into the sphere of public fears and to the top of everybody's threat list. As a result, more and more countries consider cyber attacks to be one, if not *the* major future security threat.

But how justified is this assumption? And what has Stxunet really changed in the debate?

This article aims to provide a balanced picture of the phenomenon of cyberwar. It will show how and why the meaning of "cyberwar" has evolved from the narrow conception referring exclusively to military interaction to its broad meaning, which has become detached from "war" and encompasses almost every activity linked to the aggressive use of computers. In particular, it will distinguish between different forms of cyber conflict in order to lay the ground for a levelheaded threat assessment.

Dr. Myriam Dunn Cavelty is head of the New Risk Research Unit at the Center for Security Studies in Zurich, Switzerland.

This article was first published in *Military and Strategic Affairs* 3, no. 3 (2011): 11-19.

It further shows that there is probably less change and more persistence in the cyber threat debate at large than is currently acknowledged. The threat image has been quite solid since the late 1990s, and Stuxnet has not changed this to any substantial degree. The same can be said for the countermeasures that are planned or envisaged.

Contexts and Meanings of Cyberwar

The importance and emergence of the concept of cyberwar can best be understood in the larger context of the information revolution, which has shaped – and is still shaping – perceptions of opportunities and dangers. In particular, the technologies of the information revolution and related organizational innovations in the 1980s and 1990s seemed to alter the nature of conflict and the kinds of military structures, doctrines, and strategies needed. Thus, it seemed to imply the rise of a "new" kind of warfare in which the factor of information was to grow more and more important. This development was facilitated (if not driven) by the end of the Cold War and the ensuing reorientation in terms of enemies, strategic thought, and defense spending.

It was the second Persian Gulf war of 1991 that created a watershed in military thinking about cyberwar. That conflict was seen by military strategists (mainly American) as the first of a new generation of conflicts where victory is no longer ensured only by physical force, but also by the ability to win the information war and to secure "information dominance." As a result of the conflict, strategists began to publish scores of books on the topic.[2] The reaction to the technological developments after the Gulf War also manifested itself in the publication of new doctrinal papers that institutionalized the information component.

The debate was initially characterized by a great deal of euphoria. Soon after, however, more attention was given to the risks associated with this development. Specifically, the formulation of strategies that no longer aimed at enemy capabilities but directly targeted the opponents' flow of information highlighted the relatively high vulnerability of networked US troops. As the debate over attacks on potential hostile information systems progressed, the possible dangers to civilian data networks were also increasingly discussed. The US as the only remaining superpower was seen as predestined to become the target of asymmetric warfare. Widespread fear took root in the strategic community that those likely to fail against the US war machine might instead plan to bring the US to its knees by striking against vital points at home, namely, critical infrastructures.[3] The concept of critical infrastructure includes sectors such as information and telecommunications, financial services, energy and utilities, and transport and distribution. It also includes a list of additional elements that vary across countries and over time.[4] Most of these sectors rely on a spectrum of software-based control systems for their smooth, reliable, and continuous operation.

With the growth and spread of computer networks into more and more aspects of everyday life, the object of protection moved from being perceived to be limited proprietary (governmental, mainly military) networks to encompass the whole of society – or rather, its way of life provided by the uninterrupted sub-structure of technology.[5] On this basis, a comprehensive threat image with two interrelated sides evolved. First, an inward-looking perspective sees the very connectedness of infrastructure systems as posing dangers, because perturbations within them can cascade into major disasters with immense speed and beyond our control. Advances in information and communication technology have thus augmented the potential for major disaster in critical infrastructures by vastly increasing the possibility for local risks to mutate into systemic risks. Second, an outward-looking perspective focuses on the increasing willingness of malicious actors to exploit vulnerabilities without hesitation or restraint. Because critical infrastructure systems combine symbolic and instrumental values, attacking them becomes integral to a modern logic of destruction that seeks maximum impact.

In addition, the cyber dimension reformulates space into something no longer embedded in place or presence. The "enemy" becomes a faceless and remote entity, a great unknown that is almost impossible to track. This results in two significant characteristics of the threat representation. First, the protective capacity of space is obliterated; there is no place that is safe from an attack or from catastrophic breakdown in general. Second, the threat becomes quasi universal because it is now everywhere.

A Cyber Phenomenology

It comes as little surprise, then, that cyber threats are feared the way they are. Nonetheless, every observer cannot help but notice how unspecified the threats actually are. By leaving its military confines, the concept became greatly blurred: cyberwar has come to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers.

Such conceptual vagueness is not helpful if we are to understand what goes on in "cybered" conflicts[6] and what kinds of countermeasures are actually needed for what kind of phenomena. Bruce Schneier, an internationally renowned security technologist and author, differentiates between cyber vandalism, which includes the defacing of websites; cyber crime, which includes theft of intellectual property, extortion based on the threat of Distributed Denial of Service attacks (DDoS) attacks, fraud based on identity theft, and so on; cyber terrorism, e.g., hacking into a computer system to cause a nuclear power plant to melt down, a dam to open, or two airplanes to collide; and cyberwar.[7] Schneider uses "cyberwar" to refer to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems.

Schneier's classifications construct a cyber threat escalation ladder – from rung to rung, the potential effects as well as the scope and the intensity become more severe. The last few years have shown that cyber espionage and cyber sabotage are missing from this ladder. More important, however, is that the lines of demarcation between the different activities are greatly blurred. When a particular detrimental event occurs, it is often difficult to determine whether it is the result of a malicious attack, a failure of a component, or an accident. And although their goals are different, the tools and tactics used by armies, terrorists, and criminals in cyberspace are very similar, if not the same. This means that knowing who is behind an attack and what kind of phenomenon it constitutes is a major difficulty when it occurs.

Then again, just because it is difficult does not mean that such a differentiation is not necessary: the opposite is true. First, the advantage of a "severity of effects" view is that it helps policymakers prioritize in theory, which is highly needed. Only computer attacks whose effects are sufficiently destructive or disruptive should be regarded as a national security issue – and should therefore earn the attention needed for something existentially threatening. Attacks that disrupt nonessential services or that are mainly a costly nuisance are not.[8] Second, a narrow and precise definition also helps to circumvent other dangers inherent in calling something "war," like exculpating the victims of an attack from their own responsibility for the consequences of their negligence in terms of computer security or creating pressure to retaliate against hackers, real or imagined.[9] Third, it clearly shows where the center of gravity lies: with careful computer forensics. Each and every occurrence must be carefully investigated. As Schneier notes:

> Just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar. A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime, or even – if it's done by some fourteen-year-old who doesn't really understand what he's doing – cybervandalism. Which it is will depend on the motivations of the attacker and the circumstances surrounding the attack...just as in the real world.[10]

Threat Assessment

That said, how endangered are we? Conflicts in cyberspace have been a reality for over a decade: elements of any political, economic, and military conflict take place in and around the internet. Furthermore, criminal and espionage activities aided by information and communication technologies take place every day. But in the entire history of computer networks, there have been very few examples of severe attacks that had the potential to disrupt or actually did disrupt the activities of a nation state in a major way. There are even fewer examples of cyber attacks that resulted in physical violence against persons or property. The huge majority of cyber attacks are low level and cause inconvenience rather than serious or long term disruptions. In fact, it has been convincingly shown that a "pure" (or strategic) cyberwar is very unlikely to ever occur, with attacks on computer systems more likely to be used in conjunction with other, physical forms of attack.[11]

Did this estimation change with Stuxnet? Classifying Stuxnet according to the escalation ladder is a challenge. Stories and speculations about the worm, its origins, and its intent exist by the thousands.[12] Well written or less so, they all contain bits and pieces of a puzzle that is inherently unsolvable. The pieces of the puzzle all seem to suggest that only one or several nation states – the usual "cui bono" logic pointing either to the US or Israel – would have the capability and interest to produce and release Stuxnet in order to sabotage the Iranian nuclear program. Though the world will probably never know for certain who is behind this piece of code, the majority of strategic planners out there are willing to believe that a "digital first strike" has occurred and a virtual Pandora's Box has been opened.

However, even if the most extreme case is assumed – that the majority of states in this world have developed effective and powerful cyber weapons or will in the near future (which is very doubtful) – the mere existence and availability of such capabilities does not automatically mean that they will be used. The cyber realm seems to lead people to assume that because they have vulnerabilities they will be exploited. Still, in security and defense matters, careful threat assessments need to be made. Such assessment necessitates the careful deliberation of the following question: "Who has the interest and the capability to attack us, and why would they?" For many democratic states, the risk of war has moved far to the background. The risk of a cyber attack of the severest proportions should be treated the same if there is no natural enemy.

Unraveling the Stuxnet Effect

On the other hand, the publication of Stuxnet's code and many other details has already led to many piggyback attacks. SCADA systems – computer systems that monitor and control industrial, infrastructure, or facility-based processes – are therefore likely going to be the target of choice for any kind of hacker in the near to midterm future. This comes with an inherent danger of intended and unintended (side) effects, of course – but in fact, the critical infrastructure community has been talking about the threat to SCADA systems for over a decade. In addition, experts have been expecting a major occurrence in cyberspace for a long time. Seen this way, Stuxnet is less of a surprise and more of a confirmation of what has been discussed and feared for years. Though it has focused the minds of politicians on the upper two rungs of the ladder, at least temporarily, it does not change the probability of cyber terror or cyberwar occurring.

It also does not change the methods and tools available to counter cyber threats. This concerns information assurance measures, for example, or the many diverse activities, concepts, and processes subsumed under "critical infrastructure protection" (CIP). CIP is handled similarly in many states:[13] close partnerships with the corporate sector and international partners are sought, mostly in order to exchange information on threats and issues. In addition, more recently, a shift away from the concept of protection towards the concept of "resilience" can be observed.[14] Resilience is not a new concept, of course, but its current rise indicates a significant and crucial shift in thinking. While protective (and defensive) measures aim to prevent disruptions from happening, resilience accepts that certain disruptions are inevitable.

Such thinking is absolutely necessary and needs to become rooted deeply in politicians' minds and subsequently in the minds of the population. Information networks can never be "secure" in the national security sense. In fact, the opposite is true: cyber incidents are fated to happen, because they simply cannot be avoided. In other words, even the most perfect defenses will not be able to guarantee that nothing severe will happen in a networked world.

States have the tendency to react forcefully to such a challenge and try to increase the level of security by all means. But cyberspace should not be mistaken for just another "realm" in which military action can be taken at will. To continue reaping the benefits of the cyber age, it is necessary to learn how to live with insecurity in pragmatic ways. Apart from legal and strategic restraints that will certainly be factored into any consideration of whether to use cyber attacks as weapons or not, the biggest impediment should be fears of uncontrollable blowback. First of all, repercussions could emerge directly through the interdependencies between various critical assets that characterize the environment. Second, blowback may be felt through the more intangible effect of undermined trust in cyberspace, with damaging repercussions for the global economy.[15]

By implicitly or explicitly moving an issue into the realm of national security and military actions, one tends to subject it to the rules of an antagonistic zero sum game, in which one party's gain is another party's loss. The logic of cyberspace, however, is a different one. Like the governance of space and the oceans, its governance requires globally accepted norms. The avenues currently available for arms control in this arena are primarily information exchange and norm building, whereas attempts to prohibit the means of cyberwar altogether or restricting the availability of cyber weapons are likely to fail. However, these difficulties should not prevent the international community from pushing all countries to adopt responsible limits and self-restraint in the use of cyber weapons and from thinking about new and innovative ways to enhance protection of vital computer networks without inhibiting the public's ability to live and work with confidence on the internet.

Notes

[1] John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141-65.

[2] Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001); Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington: Brookings Institution, 1999).

[3] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008).

[4] Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009* (Zurich: Center for Security Studies, 2009).

[5] Myriam Dunn Cavelty, "Cyber-Security," in Peter Burgess, ed., *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 154-62.

[6] Chris Demchak, "Cybered Conflict as a New Frontier," *Atlantic Council*, October 28, 2010, http://www.acus.org/new_atlanticist/cybered-conflict-new-frontier.

[7] Bruce Schneier, "Schneier on Security: A Blog Covering Security and Security Technology," Post: "Cyberwar," June 4, 2007, http://www.schneier.com/blog/archives/2007/06/cyberwar.html.

[8] Cf. Clay Wilson, *Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Report for Congress (Washington: Congressional Research Service, 2003) and Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001), pp. 239-88.

[9] Martin Libicki, *Defending Cyberspace and Other Metaphors* (Washington: National Defense University, 1997), p. 38.

[10] Schneier, http://www.schneier.com/blog/archives/2007/06/cyberwar.html.

[11] Peter Sommer and Ian Sommer, *Reducing Systemic Cybersecurity Risk*, OECD/IFP Project on Future Global Shocks, 2011, www.oecd.org/dataoecd/3/42/46894657.pdf.

[12] Two prominent examples are: Mark Clayton, "Stuxnet Malware is Weapon out to Destroy Iran's Bushehr Nuclear Plant," *Christian Science Monitor*, September 21, 2010, www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant; and William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[13] Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model For Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-87.

[14] Christine Pommerening, “Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm,” in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, CIP Program Discussion Paper Series (Washington: George Mason University, 2007), pp. 9-22.

[15] Andrew Rathmell, “Controlling Computer Network Operations,” *Information & Security: An International Journal* 7 (2001): 121−44.

The Threat of Terrorist Organizations in Cyberspace

Gabi Siboni, Daniel Cohen, and Aviv Rotbart

Introduction

The first motion picture ever screened before an audience was produced by the Lumiere brothers in 1895. It showed a train entering a station, seemingly moving toward the viewers in the hall. The spectators, who were convinced that the train was approaching them, screamed in panic and fled the building. During the first movie ever shown, it seemed to the spectators that what they were seeing was reality.[1]

Cyber terrorism is a field in which reality and science fiction are sometimes intertwined. If we examine one of the key concepts in cyberspace – namely, dealing with terrorist threats – we find that the rationale underlying the concept (which emerged after the formative events at the beginning of the twenty-first century, such as the Y2K bug and the September 11, 2001, terrorist attacks) is that the world appears to be at the peak of a process that belongs to the post-modern and post-technology era, an era with no defensible borders, in which countries are vulnerable to invasion via information, ideas, people, and materials – in short, an open world. In this world the threat of terrorism takes a new form: a terrorist in a remote, faraway basement has the potential ability to cause damage that completely changes the balance of power by penetrating important security or economic systems in each and every country in the world and accessing sensitive information, or even by causing the destruction of vital systems.[2]

Can the reality of September 11, 2001 – when a terrorist organization that had planned an attack for two years, including by taking pilot training

Dr. Gabi Siboni is a senior research fellow and the head of the INSS Cyber Warfare Program. Daniel Cohen is the coordinator of the Cyber Warfare Program at INSS. Aviv Rotbart is a doctoral student in the Department of Computer Science at Tel Aviv University.

This article was first published in *Military and Strategic Affairs* 5, no. 3 (2013): 3-29.

courses, eventually used simple box-cutters to carry out a massive terrorist attack – repeat itself in cyberspace? Is a scenario in which a terrorist organization sends a group of terrorists as students to the relevant courses in computer science, arms them with technological means accessible to everyone, and uses them and the capabilities they have acquired to carry out a massive terrorist attack in cyberspace realistic or science fiction? In order to answer this question, we must first consider what capabilities a non-state actor can acquire, and whether these capabilities are liable to constitute a real threat to national security. An analysis of the main threats facing a country over the course of several years, given expected changes in its strategic balance sheet, requires identifying the entities threatening a country as well as the roots of the threat and the reasons for it.

No one disputes that non-state actors, terrorist organizations, and criminals are using cyberspace for their own purposes and deriving benefit from a field in which everyone is at the same starting point – a field that also enables small individual players to have an influence disproportionate to their size. This asymmetry creates various risks that did not attract attention or provoke action among the major powers in the past. The question is whether the activity of these players in cyberspace constitutes a threat with the potential to cause major and widespread damage, and if so, why such damage has not yet occurred.

This article assesses whether attacks in cyberspace by terrorist organizations, whose effect until now has usually been tactical, will be able to upgrade (or perhaps have already upgraded) their ability to operate cyber weapons with strategic significance – weapons that can inflict large scale or lasting damage of the sort that causes critical systems to collapse and "brings countries to their knees." The purpose of this article is to discuss the threat of cyberspace terrorism and assess the truth of the concepts that have emerged in recent years concerning this threat.

This article focuses on the activities of non-state organizations with political agendas and goals, even if operated or supported by states. A distinction is drawn between these activities and those that are conducted directly by countries, which are beyond the scope of the article, as are the activities of organizations whose aims are mainly of a criminal nature. For the purposes of this article, a terrorist act of a non-state organization in cyberspace will be defined as an act in cyberspace designed to deliberately or indiscriminately harm civilians. For example, disruption of the internet site of a commercial bank by a non-state organization with political goals will be defined as an act of terrorism in cyberspace. Figure 1 illustrates the scope of discussion in this article.

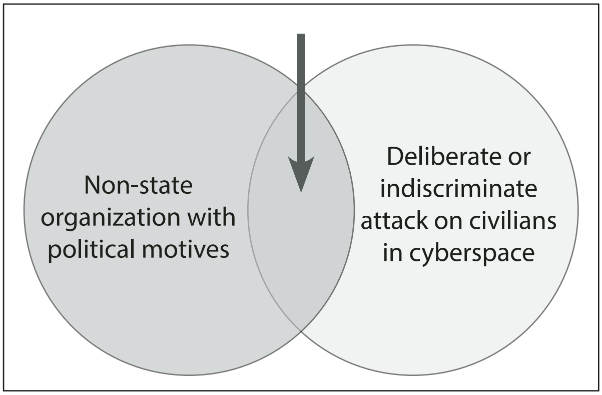
Non-state organization with political motives
Deliberate or indiscriminate attack on civilians in cyberspace

Figure 1. Terrorist Acts in Cyberspace

The Methodology of the Study

A number of benchmarks had to be met in order to assess the activity of terrorist organizations in cyberspace. The first was identification of the motives for using cyberspace as part of the political struggle being waged by the terrorist organizations. Toward this end, two principal motives were identified. The first is the use of cyberspace in support of terrorist activity, mainly the acquisition of money and recruits or money laundering in order to finance the activity. The second is the use of tools in cyberspace to provide the actual strike against the targets that the terrorist organization set for itself, as well as its use for other violent means. In this context we will analyze the cooperation between non-state organizations and the states that operate them and support their terrorist activity.

The second benchmark of this study required an assessment and in-depth understanding of the capabilities that terrorist organizations can obtain, bearing in mind that not every computer operator, even if a technological genius, can generate an effective and significant terrorist attack. In this context we also examined the assumption that significant attacks in cyberspace will continue to be confined to high-technology countries and will require considerable resources in terms of both intelligence and technology. Next, having established an understanding of the terrorist organizations' array of relevant technological and intelligence capabilities, it was necessary to consider whether such activities by terrorist organizations have actually been identified. Finally, all the findings were analyzed in order to formulate conclusive insights and recommendations as part of the defense needs.

Analysis of Capabilities

Cyberspace contributes to the enhancement of knowledge and acquisition of capabilities. In addition, technology is useful in creating an anonymous communications network.[3] Similarly, cyberspace serves as a platform for expanding the circle of partners for terrorist activity. In contrast to the recruitment of terrorist operatives in the physical world, in cyberspace it is possible to substantially enlarge the pool of participants in an activity, even if they are often deceived into acting as partners by terrorist organizations using the guise of an attack on the establishment. This phenomenon is illustrated by the attacks by hackers against Israeli targets on April 7, 2013,[4] when some of the attackers received guidance concerning the methods and targets for the attack from camouflaged Internet sites. The exploitation of young people's anti-establishment sentiments and general feelings against the West or Israel makes it possible to expand the pool of operatives substantially and creates a significant mass that facilitates cyber terror operations. For example, it has been asserted that during Operation Pillar of Defense over one hundred million cyber attacks against Israeli sites were documented,[5] and that during the campaign and the attacks there were quite a few operatives who followed developments through guidance apparently provided by Iran and its satellites.[6]

On the one hand, the array of capabilities and means at the disposal of terrorist organizations in cyberspace is limited because of its strong correlation with technological accessibility, which is usually within the purview of countries with advanced technological capabilities and companies with significant technological capabilities. On the other hand, access to the free market facilitates trade in cybernetic weapons and information of value for an attack. One helpful factor in assembling these capabilities is countries that support terrorism and seek to use proxies in order to conceal their identity as the initiator of an attack against a specific target. In addition, the terrorist organization must train experts and accumulate knowledge about ways of collecting information, attack methods, and means of camouflaging offensive weapons in order to evade defensive systems at the target.

This study reveals that to date terrorist organizations have lacked the independent scientific and technological infrastructure necessary to develop cyber tools with the ability to cause significant damage. They also lack the ability to collect high quality intelligence for operations. The ability of terrorist organizations to conduct malicious activity in cyberspace will therefore be considered in light of these constraints.

As a rule, a distinction should be drawn among three basic attack categories: an attack on the gateway of an organization, mainly its internet sites, through direct attacks, denial of service, or the defacement of websites; an attack on an organization's information systems;[7] and finally, the most sophisticated (and complex) category, attacks on an organization's core operational systems,[8] affecting its core functions – for example, industrial control systems.[9] Cyber terror against a country and its citizens can take place at a number of levels of sophistication, with each level requiring capabilities in terms of both technology and the investment made by the attacker. The damage that can be caused is in direct proportion to the level of investment.

An Attack at the Organization's Gateway

As noted, the most basic level of attack is an attack on the organization's gateway, that is, its internet site, which by its nature is exposed to the public. The simplest level of cyber terrorism entails attacks that deny service and disrupt daily life but do not cause substantial, irreversible, or lasting damage. These attacks, called "distributed denials of service" (DDOS), essentially saturate a specific computer or internet service with communication requests, exceeding the limits of its ability to respond and thereby paralyzing the service. Genuine requests go unanswered because the service is overloaded by having to deal with the attacker's requests.

DDOS attacks carried out by a terrorist organization[10] need to be effective and continue for a significant amount of time to ensure that as many people as possible become aware of the attack and are affected by the denial of service. Suitable targets for such an attack are, among others, banks, cellular service providers, cable and satellite television companies, and stock exchange services (trading and news). Popular cellular applications whose disruption can be a nuisance, such as WAZE, access to e-mail service, and appointments calendars, as well as Voice over Internet Protocol (VoIP) call applications, may be added to this list.

Another method of attacking an organization's gateway is through attacks on Domain Name System (DNS) servers – servers used to route internet traffic. Such an attack will direct people seeking access to a specific site or service towards a different site, to which the attackers seek to channel the traffic. A similar, but simpler, attack can be conducted at the level of an individual computer instead of the level of the general DNS server, meaning that communications from a single computer will be channeled to the attacker's site rather than the real site which the user wishes to surf. Damage caused by such attacks can include theft of information; denial of service to customers, resulting in business damage to the attacked service; and damage to the reputation of the service. The attacker can redirect traffic to a page containing propaganda and messages he wants to present to the public.

One popular and relatively simple method of damaging the victim's reputation at the gateway of the organization is to deface its Internet site. Defacement includes planting malicious messages on the home page, inserting propaganda that the attackers wish to distribute to a large audience, and causing damage to the organization's image (and business) by making it appear unprotected and vulnerable to potential attackers.

An Attack against the Organization's Information Systems

The intermediate level on the scale of damage in cyberspace includes attacks against the organization's information and computer systems, such as servers, computer systems, databases, communications networks, and data processing machines. The technological sophistication required at this level is greater than that required for an attack against the organization's gateway. This level requires obtaining access to the organization's computers through employees in the organization or by other means. The damage that can be caused in the virtual environment includes damage to important services, such as banks, cellular services, and e-mail.

A clear line separates the attacks described here from the threat of physical cybernetic terrorism: usually these attacks are not expected to result in physical damage, but reliance on virtual services and access to them is liable to generate significant damage nevertheless. One such example is the attack using the Shamoon computer virus,[11] which infected computers of Aramco, the Saudi Arabian oil company, in August 2012. Even though the attack did not affect the company's core operational systems, it succeeded in putting tens of thousands of computers in its organizational network out of action while causing significant damage by erasing information from the organization's computers and slowing down its activity for a prolonged period.[12]

An Attack on the Organization's Core Operational Systems

The highest level on the scale of attack risk is an attack on the organization's core operational and operating systems. Examples include attacks against critical physical infrastructure, such as water pipes, electricity, gas, fuel, public transportation control systems, or bank payment systems, which deny the provision of essential service for a given time, or in more severe cases, even cause physical damage by attacking the command and control systems of the attacked organization.

A successful offensive could cause the release of hazardous materials into the air and physical harm to a large population. This is the point at which a virtual attack is liable to create physical damage and its effects are liable to be destructive. Following the exposure of Stuxnet, awareness increased of the need to protect industrial control systems, but there is still a long way to go before effective defense is actually put into effect. Terrorist groups can exploit this gap, for example by assembling a group of experts in computers and automation of processes for the purpose of creating a virus capable of harming those systems.[13]

Another way of obtaining physical cyber weaponry is likely to emerge from the black market in cyber weapons and its expansion to include physical infrastructure, in addition to the virtual weaponry that it already offers now. It should be noted that as of the date of this writing, such a scenario has not actually occurred. Because it involves complex and costly cybernetic weaponry, however, it is possible that clandestine trading in this area is already underway in the internet underworld.[14] As noted, this is the highest level on the cyber attack scale, and the costs and damage caused by it are correspondingly high, as evidenced by the Stuxnet worm.[15]

Development of attack capabilities, whether by countries or by terrorist organizations, requires an increasingly powerful combination of capabilities for action in cyberspace in three main areas: technological capabilities, intelligence guidance for setting objectives (generating targets), and operational capacity.

Technological Capabilities

The decentralized character of the Internet makes trade in cyber weaponry easy. Indeed, many hackers and traders are exploiting these advantages and offering cyber tools and cyberspace attack services to anyone who seeks them. A varied and very sophisticated market in cyber products trading for a variety of purposes has thus emerged, with a range of prices varying from a few dollars for a simple one-time denial of service attack to thousands of dollars for the use of unfamiliar vulnerabilities and the capabilities to enable an attacker to maneuver his way into the most protected computer system. Thanks to cyberspace, this market is growing by building on the infrastructure of social networks and forums that allow anonymous communications between traders and buyers.[16] In an interesting phenomenon, seen only recently, these traders are leaving the web underground and stepping out into the light. They can be found on the most popular social network of all: Facebook.[17] A blog by information security company RSA[18] describes a new situation, in which the traders offer their wares not only as goods, but also as a complete service, including the installation of command and control servers, training in the use of the tools, and even discounts, bargains, and the option of buying only certain modules of the attack tool in order to reduce the price. The growth of this market raises the question whether and how terrorist organizations can use all the knowledge and tools that have accumulated in the cyber crime market.

In order to answer this question, it is necessary to assess the gap between the abundance of tools and capabilities currently offered for sale openly on the Internet and the requirements of terrorist organizations. Today's market for attack tools is aimed at cyber criminal organizations, mainly for purposes of fraud, stealing funds from unwitting bank account holders, and identity theft by collecting particulars from credit cards, bank account numbers, identity cards and addresses, entry passwords to financial websites, and the like. These tools are not necessarily suitable for the needs of terrorist organizations. At the same time, many terrorist organizations might engage in the practices of cyber criminal organizations for the sake of fundraising to finance their main terrorist activity. The principal objective of terrorist organizations – causing substantial damage and instilling fear – can be accomplished in a number of ways and at different levels of difficulty and severity. The tools of the cybernetic underworld can be of great assistance in DDOS attacks and in stealing large quantities of sensitive information from inadequately protected companies (for example, information about credit cards from unprotected databases), which will almost certainly arouse public anxiety. Terrorists still have a long way to go, however, before they can cause damage to control systems, which is much more difficult than stealing credit cards, and towards which cybernetic crime tools are of no help. With respect to the intermediate level described above concerning attacks on an organization's information systems, it appears that the underworld possesses tools capable of assisting cyber terrorism. Some adjustment of these tools is needed, such as turning the theft of information into the erasure of information, but this is not nearly such a long process, and the virus developers will almost certainly agree to carry it out for terrorist organizations, if they are paid enough.

Intelligence-Guided Capability

One of the key elements in the process of planning a cyber attack is the selection of a target or a group of targets, damage to which will create the effect sought by the terrorist organization. Towards this end, a terrorist entity must assemble a list of entities that constitute potential targets for attack. Technology that provides tools facilitating the achievement of this task is already available free of charge. For example, the Facebook and LinkedIn social networks can be used to find employees in the computer departments of infrastructure companies, food companies, and the like. Taking the Israel Electric Corporation as an example, academic studies[19] show that company divisions can be mapped, employees can be found in the various departments, and those with access to the company's operational systems can be selected, all with no great difficulty.[20] If these employees are aware of the importance of information security, and therefore cannot be directly attacked, their families and friends can be traced through Facebook, and the desired target can be attacked through them. Social networks constitute an important source for espionage and collection of business and personal information about companies and organizations,[21] and terrorist organizations can easily use the information distributed through them for their own benefit.

It is also necessary to map the computer setup of the attacked organization, and to understand which computers are connected to the internet, which operating systems and protective software programs are installed on them, what authorizations each computer has, and through which computers the organization's command system can be controlled. For example, if a terrorist organization wants to control the functioning of a turbine that produces electricity, its task, although much more technical and difficult than mapping the company's organizational structure, is now especially easy, following the publication of a study by a "white hat" hacker, who conducted the first "internet census" in history.[22]

Using a ramified network of robots (software programs implanted in computers that wait for an order from the command and control center to which they are connected), the white hat hacker compiled a list of 1.3 billion IP addresses in use, for some of which he published technical data such as the type of open gates, the requests to which these addresses respond, and more. The published results of the census are freely available to all interested Internet surfers. For a malicious hacker, these data are sometimes necessary in order to attack and take over the entire computer system of an individual or organization. Thus a company's organizational structure can be mapped, and if its network is not adequately protected, information can also be gleaned about the computers used by the company's employees.

Good protection and awareness of information security capabilities can make it very difficult for hackers and terrorists to carry out the abovementioned actions. Organizations with critical operational systems usually use two computer networks: one external, which is connected to the internet, and one internal, which is physically isolated from the internet and is connected to the organization's industrial control systems. The internet census does not include information about isolated internal networks because these are not accessible through the internet. Any attack on these networks requires intelligence, resources, and a major effort, and it is doubtful that any terrorist organizations are capable of carrying out such attacks. Here the terrorist organizations can take advantage of another study conducted by hackers from the University of Berlin,[23] which uses a Google map (enabling researchers to present and share geographic information that they have collected) to display a large number of industrial control systems (ICS) deployed throughout the world that are connected to the internet. The information displayed on the map is taken from an enormous database freely available to everyone through the Shodan website,[24] which makes the life of a terrorist hacker much easier. This service uses information collected by Google for its mapping and location-based advertising services and makes it accessible to the public. It is possible that the hackers who recently broke into the home networks of hundreds of Israelis used services from the Shodan website in order to collect intelligence for the attack, and perhaps also to obtain tools (cyber ammunition) to actually carry it out.[25]

Operational Capability

After collecting intelligence and creating or acquiring the technological tools for an attack, the next stage for planners of cybernetic terrorism is operational – to carry out an actual attack by means of an attack vector.[26] This concept refers to a chain of actions carried out by the attackers in which each action constitutes one step on the way to the final objective, and which usually includes complete or partial control of a computer system or industrial control system. No stage in an attack vector can be skipped, and in order to advance to a given step, it must be verified that all the preceding stages have been successfully completed.

The first stage in an attack vector is usually to create access to the target. A very common and successful method for doing this in cyberspace is called spoofing, that is, forgery.[27] There are various ways of using this method, with their common denominator being the forging of the message sender's identity, so that the recipient will trust the content and unhesitatingly open a link within the message. For example, it is very easy to send an e-mail message to an employee at the Israel Electric Corporation (mentioned above), in which the sender forges the address of a work colleague, a relative, or another familiar person. The attacker's objective in this case is to make the receiver of the message trust the content of the message and open its attachments or enter the internet addresses appearing in it.

The forging of e-mail is an attack method that has existed for many years. Defensive measures have accordingly been developed against it, but attackers have also accumulated experience. Incidents can now be cited of completely innocent-looking e-mail messages that were tailored to their recipients, containing information relating to them personally or documents directly pertaining to their field of business. The addresses of the senders in these cases were forged to appear as the address of a work colleague. As soon as the recipients opened the e-mail, they unknowingly infected their computers with a virus.

The forgery method can be useful when the target is a computer connected to the internet and messages can be sent to it. In certain instances, however, this is not the case. Networks with a high level of protection are usually physically isolated from the outside world, and consequently there is no physical link (not even wireless) between them and a network with a lower level of security. In this situation the attacker will have to adopt a different or additional measure in the attack vector – infecting the target network with a virus by using devices that operate in both an unprotected network and in the protected network. One such example is a USB flash drive ("Disk on Key" or "memory stick"), which is used for convenient, mobile storage of files. If successful, the attacker obtains access to the victim's technological equipment (computer, PalmPilot, smartphone), and the first stage in the attack vector – creating access to the target – has been completed. Under certain scenarios, this step is the most important and significant for the attacker. For example, if the terrorist's goal is to sabotage a network and erase information from it, then the principal challenge is to gain access to the target, that is, access to the company's operational network. The acts of erasure and sabotage are easier, assuming that the virus implanted in the network is operated at a sufficiently high level of authorization. Under more complex scenarios, however, in which the terrorist wishes to cause significant damage and achieve greater intimidation, considerable investment in the stages of the attack vector is necessary, as described below.

Lockheed-Martin, which fell victim to a cyber attack, offers a methodology for analyzing cyberspace attack operations, which it calls "the Cyber Kill Chain."[28] According to this methodology, a complex cyber attack comprises seven milestones, paralleling the actions of planning the operation and creating the attack vector. The first step entails collecting intelligence about the target. The right cyber weapon for the attack must then be selected and launched at the target. The next stage includes the exploitation of a vulnerability in the target computer that will make it possible to implant a malicious file on its system, followed by installing the tool in a way that will enable it to carry out operations within the system. The stage after that is to create communications between the tool and the attacker's command and control servers, so that the tool can be guided and a report obtained from it about events on the victim's computer. The final step in the cyber kill chain is the conducting of active operations from within the victim's computer, such as erasure, spreading of the tool, taking over the physical devices accessible from the computer, and the like. The term "Cyber Kill Chain" was chosen in order to emphasize that in order for the attacker to succeed in carrying out a cyber attack, he must successfully complete every milestone without being detected and without his access to the target being blocked.

A terrorist organization seeking to attack operational systems will have to carry out all the stages in the chain. These are advanced and complex operations, which terrorist organizations usually do not know how to implement by themselves. If the target is protected at a very low level, no great technological capability will be required of the attacker in order to create damage or achieve defacement. In most cases, however, the terrorists will have to acquire products or services from expert hackers. In other words, they will have to use "outsourcing."

Within the offensive cyber products market, terrorists will find accessible capabilities for a non-isolated target. In the same market, they will also find attack products, and presumably they will likewise find products for conducting operations on the target network (similar to the management interface of the SpyEye[29] Trojan Horse). Despite this availability, internet-accessible tools have not yet been identified for facilitating an attack on an organization's operational systems. Access to these tools is possible in principle,[30] but the task requires large-scale personnel resources (spies, physicists, and engineers), monetary investment (for developing an attack tool and testing it on real equipment under laboratory conditions), and a great deal of time in order to detect vulnerabilities and construct a successful attack vector.

Types of Cyberspace Attacks

It is possible to identify a number of types of cyberspace attacks in accordance with both their level of expected damage and the scope of their intelligence, technological, and operational investment. In most cases, these two measures correspond with each other. The following review paints a picture of the capabilities of a non-state organization in cyberspace.

Amateur Attack

This action is taken using tools that are (in most cases) known to information security companies and are identifiable by standard protection software programs. Defenses against these tools have been developed, and they are therefore likely to prove effective only against unprotected targets. Such tools are usually used only for research or gaming purposes because only in rare cases can they be used to steal valuable information or to sabotage protected computer networks. They have spy and sabotage capabilities, but these are not very sophisticated.

Minor Attack

This is an attack in which not much effort has been invested. Most of its activity consists of searching on the internet for readymade tools or purchasing them from companies that specialize in them. Attacks of this type do not usually succeed in causing damage to entities that are attentive to information security (state, military, and advanced industrial entities), but they can penetrate private computers, steal information, and sabotage them. In most cases, these attacks are one-time events (theft of an important file, erasing a disc drive), but they can also sometimes be part of an extensive attack, such as the theft of a computer's domain name system (DNS), which makes it possible to monitor its activity on the internet.

The tools used in a minor attack do not include the various software modules; they have a single inexpensive code component that carries out all the actions of the tool. This code component is written in a way that will not allow its capabilities to be easily altered or expanded, and it is target oriented. Through the internet anyone can obtain this type of limited-capability cyber weapon for a few thousand dollars at most.

This category also includes the use of botnet software agents for DDoS attacks. Creating the network is a more complex operation, but once it is created, it can be used for many DDoS operations. It can also be leased to others for denial of service from various websites lacking high-level protection against such an attack.

Medium-Level Attack

This is an attack capable of causing significant damage or carrying out advanced spy operations at a lower cost than that of a major attack (see below). Usually this operation does not use new, unique vulnerabilities (because these are very expensive); rather, it uses known or partially known vulnerabilities against which the target is not yet protected. The operation does not include expensive modules for implementation and testing such as those developed for Stuxnet. At the same time, by using modules for an attack on computer systems (erasure, disruption) and spy modules, such an operation can be very effective as part of a short-term attack for destructive purposes (because no effort will be made to conceal the destruction, which would be too expensive) or to spy on a victim whose systems do not have high-level protection.

A medium-level attack is much less costly than a major attack, as the former entails fewer man-years and does not require special, expensive hardware or the purchase of new and expensive vulnerabilities. An inexpensive vulnerability is sufficient for penetration of the victim's computer systems, bearing in mind that these are liable to be detected and blocked in the near future. The mid-level category also includes viruses capable of spreading throughout the computer network (worms) and waiting for an order from their operator. This attack model is particularly useful in creating a network of software agent robots for DDoS operations. This category also includes a DDoS attack against protected websites, which requires sophistication from the attacker and familiarity with the protection system at the target.

Major Attack

This is an attack into which many personnel, computer, and monetary resources have been invested, and which has been thoroughly tested in the laboratory before being put into operation. This operation uses unfamiliar vulnerabilities, giving the attacker a long time to operate it before it is detected and shut down. The operation is usually camouflaged in order to leave few footprints. The software tool contains a number of modules, some of which are likely to be designed to sabotage the victim's special-purpose software or hardware systems (e.g., Stuxnet), and will never operate elsewhere, in order to reduce the possibility of detection.

A major attack operation is likely to entail a wide range of modules corresponding to the target it was designed to attack, such as spy modules – searching for files or information and sending the findings to the operator – and attack and camouflage modules – sabotaging centrifuges while misleading the control system, so that the latter will report that the former are in good repair. Such an attack involves many man-years, advanced computer resources, and sometimes hardware systems and testing equipment designed to simulate the theater in which the hostile code will operate, for example centrifuges with Siemens control systems in the case of Stuxnet.

Table 1 summarizes the differences among the various categories of cyber attack by listing the criteria that make it possible to distinguish clearly between types of cyber weapons according to the level of their capabilities. The parameters are divided into several categories. The first includes the cyber weapon envelope and its ability to reach its target and operate freely there without being blocked. The first two parameters are included in this category. Their importance lies in the comfortable work environment that they enable the attacker to enjoy, in the knowledge that he can penetrate his targets and carry out operations there whenever and however he requires, without fearing that his capability will be blocked or his weapon exposed and removed. The next three parameters constitute the second category, which pertains to the cyber weapon's ability to carry out its main activity at the target, whether that be the theft of information, its destruction, or electronic or physical damage or disruption. The various weapons in this category are distinguishable by the algorithms that they apply in order to spy on the target, and by their ability to disrupt computer and physical systems. The ability to cause physical damage constitutes the highest level in this category. The final category represents the two parameters relating to the tool's behavior within the target's network, and the extent of its capability and the freedom that it grants to its operators to conduct the operation at the target. High-level capabilities in this category are those that make it possible to adjust the weapon by delivering modules from a distance and to change the definitions of the task, send orders to the tool, and define new intelligence targets for it. Sophisticated tools will also be able to manage a large data-collection operation on the target's network by spreading to other computers and collecting concentrated and coordinated information from them.

Table 1. Differences among Cyber Attacks

	Major Attack	Medium-Level Attack	Minor Attack	Amateur Attack
Ability to penetrate systems	Very good	Good	Good	Poor
Ability to camouflage activity	Very good	Good	Mediocre	Poor
Spy capabilities	Very good	Very good	Good	Mediocre
Ability to damage computer systems	Very good	Very good	Good	Poor
Ability to damage physical systems connected to the computer setup	Good	Poor	Poor	Poor
Ability to spread	Very good	Good	Poor	Poor
Ability to communicate with a control server	Very good	Good	Mediocre	Poor

The table indicates that the criteria significantly distinguishing major attack capabilities (which few countries possess) from other cyber attack capabilities are the ability to spread on the network, to communicate with the control server, and to damage physical systems connected to the computing systems. These operations require the greatest sophistication in conducting cyber attacks. Only a few countries have access to the knowledge and the ability to produce a weapon of this type. The "minor attack" column in the table reflects the low entry level to the cyberspace battlefield. It appears that even small weapons in the hands of non-state entities are capable of penetrating computer networks well, performing espionage at a very high level, and if they are designed for it, also sabotaging the computer system that they have penetrated. Because their camouflage capability is mediocre, they are unable to reside in the attacked system for as long as heavy or medium weapons, and will therefore have to achieve their objectives within a short time.

Activities in Cyberspace Attributed to Terrorist Organizations

This section examines terrorist operations in cyberspace in accordance with the above delineation, that is, operations whose purpose is to cause deliberate or indiscriminate harm to civilians through action in cyberspace by non-state organizations with political agendas and goals, even if operated or supported by states.

One of the first documented attacks by a terrorist organization against state computer systems was by the Tamil Tigers guerilla fighters in Sri Lanka in 1998. Sri Lankan embassies throughout the world were flooded for weeks by 800 e-mail messages a day bearing the message, "We are the Black Internet Tigers, and we are going to disrupt your communications systems." Some assert that this message affected those who received it by sowing anxiety and fear in the embassies.[31] Several years later, on March 3, 2003, a Japanese cult name Aum Shinrikyo ("Supreme Truth") conducted a complex cyber attack that included the obtaining of sensitive information about nuclear facilities in Russia, Ukraine, Japan, and other countries as part of an attempt to attack the information security systems of these facilities. The information was confiscated, and the attempted attack failed before the organization managed to take action.[32]

An attack through an emissary took place in January 2009 in Israel. In this event, hackers attacked Israel's internet structure in response to Operation Cast Lead in the Gaza Strip. Over five million computers were attacked. It is assumed in Israel that the attack came from countries that were formerly part of the Soviet Union and was ordered and financed by Hizbollah and Hamas.[33] In January 2012, a group of pro-Palestinian hackers calling itself "Nightmare" caused the Tel Aviv Stock Exchange and the El Al Airlines websites to crash briefly and disrupted the website activity of the First International Bank of Israel. Commenting on this, a Hamas spokesman in the Gaza Strip said, "The penetration of Israeli websites opens a new sphere of opposition and a new electronic warfare against the Israeli occupation."[34]

The civil war in Syria has led to intensive offensive action by an organization known as the Syrian Electronic Army (SEA) – an internet group composed of hackers who support the Assad regime. They attack Syrian opposition groups using techniques of denial of services and information, or break into websites and alter their content. The group has succeeded in conducting various malicious operations, primarily against Syrian opposition websites, but also against Western internet sites. SEA's most recent action was aimed mainly against media, cultural, and news websites on Western networks. The group succeeded in breaking into over 120 sites, including *Financial Times*, *The Telegraph*, *Washington Post*, and *al-Arabiya*.[35] One of the most significant and effective attacks was in April 2013, when the Syrian Electronic Army broke into the Associated Press's Twitter account, and implanted a bogus "tweet" saying that the White House had been bombed and the US president had been injured in the attack. The immediate consequence of this announcement was a sharp drop in the US financial markets and the Dow Jones Industrial Average for several minutes.[36] The SEA is also suspected of an attempt to penetrate command and control systems of water systems. For example, on May 8, 2013, an Iranian news agency published a photograph of the irrigation system at Kibbutz Sa'ar.[37]

During Operation Pillar of Defense in the Gaza Strip in 2012 and over the ensuing months, the Israeli-Palestinian conflict inspired a group of hackers calling itself "OpIsrael" to conduct attacks[38] against Israeli websites in cooperation with Anonymous. Among others, the websites of the Prime Minister's Office, the Ministry of Defense, the Ministry of Education, the Ministry of Environmental Protection, Israel Military Industries, the Israel Central Bureau of Statistics, the Israel Cancer Association, the President of Israel's Office (official site), and dozens of small Israeli websites were affected. The group declared that Israel's violations of Palestinian human rights and of international law were the reason for the attack.

In April 2013, a group of Palestinian hackers named the Izz ad-Din al-Qassam Cyber Fighters, identified with the military section of Hamas, claimed responsibility for an attack on the website of American Express. The company's website suffered an intensive DDoS attack that continued for two hours and disrupted the use of the company's services by its customers. In contrast to typical DDoS attacks, such as those by Anonymous, which were based on a network of computers that were penetrated and combined into a botnet controlled by the attacker, the Izz ad-Din al-Qassam attack used scripts operated on penetrated network servers, a capability that allows more bandwidth to be used in carrying out the attack.[39] This event is part of an overall trend towards the strengthening of Hamas's cyber capabilities, including through enhancing its system of intelligence collection against the IDF and the threat of a hostile takeover of the cellular devices of military personnel, with the devices being used to expose secrets.[40]

Independent Cyber Attacks by Terrorist Organizations

Our analysis of attacks by terrorist organizations in cyberspace reveals that the low entry threshold for certain attacks and the access to cybernetic attack tools have not led the terrorist organizations to switch to attacks with large and ongoing damage potential. Until now, the terrorist organizations' cyber attacks have been mainly against the target organization's gateway. The main attack tools have been denial of service attacks and attacks on a scale ranging from amateur to medium level, primarily because the capabilities and means of terrorist organizations in cyberspace are limited. To date they have lacked the independent scientific and technological infrastructure necessary to develop cyber tools capable of causing significant damage. Given that terrorist organizations lack the ability to collect high quality intelligence for operations, the likelihood that they will carry out a significant cyber attack appears low.

In order for a terrorist organization to operate independently and carry out a significant attack in cyberspace, it will need a range of capabilities, including collecting precise information about the target, its computer networks, and its systems; purchasing or developing a suitable cyber tool; finding a lead for penetrating an organization; camouflaging an attack tool while taking over the system; and carrying out an attack in an unexpected time and place and achieving significant results. It appears that independent action by a terrorist organization without the support of a state is not self-evident. The same conclusion, however, cannot be drawn for organizations supported and even operated by states possessing significant capabilities.

There is also the possibility of attacks by terrorist organizations through outsourcing. A review of criminal organizations reveals that they have made significant forward strides in recent years. The Kaspersky laboratory recently exposed a new group of attackers, apparently commissioned by criminal organizations or by a state for industrial espionage purposes. This is a group of hackers named "Icefog" that concentrates on focused attacks against an organization's supply chain (using a hit-and-run method), mainly in military industries around the world.[41] Another development is the distribution of malicious codes using the crime laboratories of the DarkNet network, which has increased access to existing codes for attack purposes. Criminal organizations are already using the existing codes for attacks on financial systems by duplicating them and turning them into mutation codes.[42]

There is a realistic possibility that in the near future terrorist organizations will buy attack services from mercenary hackers and use mutation codes based on a variation of the existing codes for attacking targets. This possibility cannot be ignored in assembling a threat reference in cyberspace for attacks on the gateway of an organization or even against its information systems. It is therefore very likely that terrorist organizations will make progress in their cybernetic attack capabilities in the coming years, based on their acquisition of more advanced capabilities and the translation of these capabilities into attacks on organizations' information systems (not only on the organization's gateway).

The ability to carry out an attack that includes penetration into the operational systems and causes damage to them is quite complex. The necessity for a high level of intelligence and penetration capabilities, which exist in only a limited number of countries, means that any attack will necessarily be by a state. For this reason no successful attack by a non-state player on the core operational systems of any organization whatsoever has been seen to date. Although no such attack has been identified yet, there is a discernible trend towards improvement of the technological capabilities of mercenaries operating in cyberspace for the purposes of crime and fraud. Presumably, therefore, in exchange for suitable recompense, criminal technological parties will agree to create tools that can carry out attacks on the core operational systems of critical infrastructure and commercial companies. These parties will also be able to put their wares at the disposal of terrorist organizations.

Recommendations for Measures at the National Level

The range of threats in cyberspace is extensive. Basic defenses against these threats need not substantively distinguish among the sources of threats. The notion that a defense can be devised in cyberspace specifically against threats from terrorist groups therefore appears impractical. On the contrary, the defense concept for threats of attacks in cyberspace by terrorist organizations does not, and cannot, differ substantially from an overall defense approach to threats in this realm.

The fundamental concept for defense against cyber threats must be based on a number of basic elements: intelligence, a multi-layer defense approach, an attack approach, public awareness, and civilian defense.

Intelligence

The first basic element in defending against cyber threats is intelligence, including collection of intelligence based on guidance that takes situation assessments into account. In this context, it is important to identify threats and guide the parties collecting the intelligence with respect to information concerning terrorist groups seeking to operate in cyberspace. As noted, in many cases states are behind the activity of terrorist organizations, and intelligence gathered in the state context can also provide information for the terrorist organizations affiliated with or operated by it.

Intelligence constitutes an essential element, second to none, in dealing with threats in cyberspace. The ability to collect and analyze a large amount of information makes it possible today to create high quality intelligence both at the state level and, in more than a few cases, at the level of organizations and businesses that regularly monitor their information and communications networks for the purpose of detecting anomalous behavior that might indicate a future attack, or in order to discern irregular activity on the computer network. In this context, it is appropriate to emphasize that when a country – such as Iran – supports and sometimes even operates terrorist organizations, Western intelligence organizations should monitor not only the target country but also the organizations affiliated with it. In the context of Iran, this means monitoring Hizbollah, Hamas, and the "Syrian Electronic Army."

A Defensive Approach Containing Several Layers

This measure entails a perimeter defense as well as protection of critical assets, including the ability to maintain activity even after penetration by malicious code, and preemptive action against active parties, for example by disclosing intelligence information to law enforcement authorities in countries where the activity is taking place, or using legal tools in other countries. Such action could possibly disrupt the ability to operate the malicious code before it is distributed.

An Offensive Approach to Threats

This element in dealing with cyber threats includes two levels. The first pertains to the ability to take offensive action within – and sometimes also outside of – cyberspace through a preemptive strike against a terrorist organization's cyber resources (infrastructure, financing, websites, and operatives). The second level concerns the ability to conduct retaliatory actions after the attack, and after satisfactory identification of the parties responsible for the attack. Such a strike need not be confined to cyberspace; it can also include real physical elements. In some cases, a legal arrangement for the offensive activity is necessary in order to make the approach effective.

In more than a few cases, a chain of operations can be identified if states (such as Iran) operate non-state organizations (such as Hizbollah and SEA), when all together they operate interested parties or even deceived parties within a network for the sake of bolstering their attack capabilities. The need to operate a broad system of attackers requires guidance in a number of contexts. The first involves determining the targets to be attacked, the second concerns the timing of the attacks, and the third pertains to the tools for carrying out the attacks. All of these require the establishment of websites and special forums to which the information is channeled. This activity creates vulnerabilities by enabling disruptive and deceptive action, thereby sowing confusion while softening the impact of the attack planned by its leaders.

Explanatory Activity

It can be assumed that explanatory activity will not be effective within the very hard core of cyber attack operatives. Preventative explanatory activity has two purposes. The first is to increase awareness of the possibility that attackers are liable to be harmed as a result of preemptive activity in the country in which they reside (for example, their exposure to law enforcement authorities in that country). The second is the exposure of those behind the organization. As noted, in many cases, the attackers have been deceived and are completely unaware that they are being operated by states and terrorist organizations. It is therefore possible that these actions can reduce the scope of the phenomenon to some extent.

Organizing Civilian Defense in Cyberspace

The vulnerabilities of the civilian cyber apparatus in Israel constitute a defensive gap inviting terrorist organizations to take advantage of it. The relatively weak defenses of these systems enable terrorist organizations to take simple action against targets in this sphere. Since civilian cyber systems create structural vulnerabilities, a civilian defense should be established in cyberspace, and the sooner the better. The recommendation of the Institute for National Security Studies to the Israeli government is that the defense of civilian cyberspace should be formulated so that it can provide a better solution to threats should be noted in this context.[43]

Terrorist organizations have not yet crossed the operational and technological threshold that would allow them to operate independently against Israel and other Western countries in the cyber warfare sphere. Developments in the criminal attack market, however, are liable to produce significant attack capabilities. These developments, combined with the support and guidance in intelligence and operations provided by technological powers like Iran, could lead to dangerous activity in the cyber field on the part of terrorist organizations. This threat, therefore, should not be taken lightly. Even though no significant activity by terrorist organizations in the cyber field has been observed yet, the development of the threat in this sphere requires appropriate organization.

Notes

[1] The authors would like to thank Noam K. from the National Cyber Staff and Doron Avraham and Keren Hatkevitz, interns in the Cyber Warfare Program at the INSS, for their assistance in preparing this article. Michal Aviad, *Documentary Film* (Tel Aviv: Heidekel, 2007), p. 5.

[2] For example, see Haim Pass and Dan Meridor, eds., *21st Century Battle: Democracies Fight Terrorism, Study Forum* (Jerusalem: Israel Democracy Institute, 2006), p. 25.

[3] For example, see Tor – a software program that helps create anonymity on the web. Every layer is encoded, and every station in the route folds its layer and delivers it to the next station. This principle is called an "onion router," https://www.torproject.org.

[4] Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April," *Haaretz*, March 14, 2013, http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214.

[5] "Steinitz: Military Threat against Israel has also Become a Cyber Terror Threat," *Globes*, July 9, 2013, http://www.globes.co.il/news/article.aspx?did=1000860690.

[6] See the statement by Prime Minister Benjamin Netanyahu on this subject: "Netanyahu: Iran and Its Satellites Escalating Cyber Attacks on Israel," *Globes*, June 9, 2013 http://www.globes.co.il/news/article.aspx?did=1000851092.

[7] This refers to any system for storing, transporting, or processing organizational information, whether or not it is connected to the internet, and whether or not it constitutes part of the organization's core business.

[8] An organization's core operational system is the hardware on which the organization's core processes are managed and the software used for that purpose (whether it is a security or a civilian business organization). Disruption or destruction of such a system can halt all or part of the organization's activity and could cause physical damage in certain cases.

[9] An industrial control system (ICS) is a tool that integrates software and hardware components and is designed to oversee a physical production

process. The system contains sensors for monitoring the controlled process and inspectors who control this process. The system is also likely to include a connection to the organization's other computer networks and sometimes also to the internet.

10 This type of attack is also carried out independently by activists and anarchists, or on behalf of and guided by a terrorist organization.

11 "Shamoon Virus Targets Energy Sector Infrastructure," *BBC News Technology*, August 17, 2012, http://www.bbc.co.uk/news/technology-19293797.

12 In this incident, malicious code was inserted into Aramco's computer system, and 30,000 computers were put out of action as a result.

13 Ralph Langner, lecture on the subject of securing industrial control systems, Annual Cyber Conference, Institute for National Security Studies, September 4, 2012, http://youtube/sBsMA6Epw78.

14 "The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Ply their Trade on the Internet," *Daily Mail*, October 11, 2013, http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html.

15 Jesse Emspak, "Why We Won't Soon See another Stuxnet Attack," *Tech News Daily*, July 24, 2011, http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html.

16 Aditya K. Sood and Richard J. Enbody, "Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market," *International Journal of Critical Infrastructure Protection* 6, no. 1, (March 2013), http://www.sciencedirect.com/science/article/pii/S1874548213000036.

17 A Facebook page offering cyber weapons for sale can be found at https://www.facebook.com/groups/53807916899/.

18 Limor Kessem, "Zeus FaaS Comes to a Social Network near You," *RSA, Speaking of Security*, April 2013, http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/.

19 Michael Fire, Rami Puzis, and Yuval Elovici, "Organization Mining Using Online Social Networks," *arXiv:1303.3741* .

20 Aviad Elishar, Michael Fire, Dima Kagan, and Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots," International Workshop on Social Network Analysis in Applications (SNAA), August 2013.

21 Fernando M. Pinguelo, Bradford W. Muller, Norris McLaughlin, and P.A. Marcus, "Is Social Media a Corporate Spy's Best Friend? How Social Media Use May Expose Your Company to Cyber-Vulnerability," *Bloomberg Law*, http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/.

22 Internet Census 2012, Carna Botnet, http://internetcensus2012.bitbucket.org/paper.html.

23 Map of SCADA systems in the world, http://goo.gl/maps/nqnan.

24 The Shodan website, which contains information useful to hackers: http://www.shodanhq.com/.

25 Gili Cohen, "Hackers Attack Home Networks of Hundreds of Israelis," *Haaretz*, September 11, 2013, http://www.haaretz.co.il/misc/2.444/.premium-1.2117098.

26 Attack vector: http://searchsecurity.techtarget.com/definition/attack-vector.

27 Spoofing attack: http://www.webopedia.com/TERM/S/spoof.html.

28 Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): p. 80.

29 Doug Macdonald, "A Guide to SpyEye C&C Messages," *Fortinet*, February 15, 2011, http://blog.fortinet.com/a-guide-to-spyeye-cc-messages.

30 Thomas Rid, "Cyber-Sabotage Is Easy," *Foreign Policy*, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa.

31 Dorothy E. Denning, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S House of Representatives, May 23, 2000, p. 269, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

32 For a chronology of the Aum Shinrikyo actions, see http://cns.miis.edu/reports/pdfs/aum_chrn.pdf.

33 Paul Everard, "NATO and Cyber Terrorism," in *Response to Cyber Terrorism*, (Ankara, Turkey: Center of Excellence Defence against Terrorism, 2008), pp.118-126.

34 Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," *Military and Strategic Affairs* 5, no. 1 (2013): 59-80 .

35 Dylan Love, "10 Reasons to Worry about the Syrian Electronic Army," *Business Insider*, May 22, 2013, http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P.

36 Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," *The Telegraph*, April 23, 2013. http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

37 Yanir Yagna and Oded Yaron, "Israeli Expert Said, 'Syrian Electronic Army Attacked Israel' – and Denied It," *Haaretz*, May 25, 2013, http://www.haaretz.co.il/news/politics/1.2029071.

38 Amir Buhbut, "Cyber Attack: Prime Minister's Office, Ministries of Defense, Education Websites Put out of Action," *Walla News*, April 7, 2013, http://news.walla.co.il/?w=/90/2630896.

39 Nimrod Zook, "Cyber Attack: Izz ad-Din al-Qassam Fighters Hit American Express," *Calcalist*, April 2, 2013, http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html.

40 Lee Yaron, "Defense Department Warns: Hamas Cyber Capabilities Stronger," *Bamahane*, November 14, 2013, p. 19.

41 "Kaspersky Lab Exposes 'Icefog': A new Cyber-espionage Campaign Focusing on Supply Chain Attacks," September 26, 2013, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks.

42 For more on mutation codes, see Cohen and Rotbart, "The Proliferation of Weapons in Cyberspace."

43 Gabi Siboni, "A National Response to Civil Defense in Cyberspace," Viewpoint Paper for Decision-Makers, Institute for National Security Studies, April 2013, http://heb.inss.org.il/index.aspx?id=4354&articleid=5904.

The INSS Cyber Program

The Institute for National Security Studies (INSS), an independent, nonpartisan think tank that is an external institute of Tel Aviv University, deals with issues related to Israel's national security. The Institute holds seminars, forums, and conferences and produces various publications, including monographs, journals, analytical articles, and position papers for decision makers. In 2013, INSS was ranked as Israel's leading think tank and among the leading think tanks in the world in the field of national security. INSS is a public benefit company.

The INSS Cyber Program aims to cultivate knowledge on cyber warfare and broaden the study of its related aspects. It focuses on the conceptualization and creation of a common language regarding cyberspace and national security; development and examination of national policy; and the identification of guidelines for doctrine of cyber warfare for Israel, at both the national and inter-organizational levels. Research aims to contribute to an informed public debate on cyber security and promote strong public policy on the issue.

To this end, the program engages in a variety of research activities in subjects relevant to the field of cyberspace, including: development of a national defense concept for cyberspace; sharing of knowledge and information across organizations and sectors; intelligence and operations in cyberspace; proliferation of malicious codes in the cyber sphere; terrorist and non-state organizations in cyberspace; activities by major states and other actors in cyberspace; and legal and regulatory aspects. In addition, the program publishes a bi-weekly review of cyber intelligence on the basis of open sources. This review, published in English, is distributed by the Cyber Security Forum Initiative (CSFI) as well as through other frameworks.

In order to sharpen the common language and cultivate knowledge, the Cyber Program has established a national professional forum to formulate strategic insights and policy recommendations concerning cyber defense. This forum enables the building of innovative knowledge and connections among the relevant players in both the private and public sector. In addition, it provides decision makers with an important professional resource that researches new issues in the field and publishes position papers.

Forum members include some twenty-five senior figures from three main sectors: government, the defense industry, and research and development in leading technology companies and academia. The forum holds discussions on a regular basis on a range of subjects, including: conceptualization and creation of a common language in national security contexts; development and examination of a national policy for cyber defense; the interface between the techno-tactical and strategic realms; the interface between the defense sector and the business sector; the boundaries of responsibility between the state and the private sector (organizations and individuals); and knowledge sharing and regulation.

The forum was established in an effort to narrow the gap in the discourse between two realms: the technological, home to many players and where a great deal of knowledge has developed in Israel (and the rest of the world); and the strategic, with an emphasis on Israel, where there is a need for significant improvement in the development of knowledge and policy. Thus a major aspect of the forum's role and its added value in activity and knowledge development in the cyber field in Israel is the connection it forges between the two arenas. Furthermore, the discussion underway in the context of the forum is necessary to achieve the supreme goal: a strong and lasting improvement in Israel's cyber resilience.

In 2013, partly as a result of insights that emerged from the forum's discussions, INSS published recommendations for decision makers concerning the organization of civil defense in cyberspace in Israel. One of the forum's goals during 2014 is to examine the national concept and to make recommendations for decision makers in this field.

INSS Cyber Program Team

Program Director: Dr. Gabi Siboni
Program Coordinator: Daniel Cohen
Cyber Forum Manager: Hadas Klein

Researchers
Prof. Amir Averbuch
Dr. Tal Koren
Dr. Yair Oppenheim
Major M. (IDF – C^4I Corps)
Hila Adler
Carmit Valensi

Research Assistants and Interns
Eddo Bar
Roxana Bogdanski
Giorgio Bonadiman
Nir Carmi
Keren Hatkevitz
Sarah Kohne
Sami Kronenfeld
Danielle Levin
Ran Levy
Jeremy Makowski
Amir Steiner
Simon Tsipis
Shlomi Yaas

INSS Memoranda, 2013 – Present

No. 134, March 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad*.

No. 133, March 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues* [Hebrew].

No. 132, January 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad* [Hebrew].

No. 131, December 2013, Amos Yadlin and Avner Golov, *Regime Stability in the Middle East: An Analytical Model to Assess the Possibility of Regime Change*.

No. 130, December 2013, Yehuda Ben Meir and Olena Bagno-Moldavsky, *The Voice of the People: Israeli Public Opinion on National Security 2012* [Hebrew].

No. 129, July 2013, Zvi Magen and Vitaly Naumkin, eds., *Russia and Israel in the Changing Middle East*.

No. 128, June 2013, Ruth Gavison and Meir Elran, eds., *Unauthorized Immigration as a Challenge to Israel* [Hebrew].

No. 127, May 2013, Zvi Magen, *Russia in the Middle East: Policy Challenges*.

No. 126, April 2013, Yehuda Ben Meir and Olena Bagno-Moldavsky, *The Voice of the People: Israeli Public Opinion on National Security 2012*.

No. 125, March 2013, Amos Yadlin and Avner Golov, *Regime Stability in the Middle East: An Analytical Model to Assess the Possibility of Governmental Change* [Hebrew].