Military and Strategic Affairs

Volume 4 | No. 3 | December 2012

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

Military and Strategic Affairs

Volume 4 | No. 3 | **December 2012**

CONTENTS

Military and
Strategic Affairs

The purpose of *Military and Strategic Affairs* is to stimulate and enrich the public debate on military issues relating to Israel's national security.

Military and Strategic Affairs is a refereed journal published three times a year within the framework of the Military and Strategic Affairs Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Graphic Design: Michal Semo-Kovetz, Yael Bieber
Tel Aviv University Graphic Design Studio

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 61398 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Military and Strategic Affairs is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

A Blueprint for Cyber Deterrence: Building Stability through Strength

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

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

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

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

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

State Actors

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

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

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

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

Non-State Actors

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

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

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

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

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

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

Contours of the Cyber Threat

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Evans has reasoned further as follows:

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

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

Cyber Deterrence and Multidimensional Response

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Building Stability through Strength

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Notes

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

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

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

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

5 Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

44 *The Book of Five Rings.*

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

46 Ibid.

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

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

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

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

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

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

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

54 Cilluffo, *AFPC Defense Dossier*.

On Nuclear War: Deterrence, Escalation, and Control

Stephen J. Cimbala

Introduction

During the Cold War, and especially in the 1980s, there were some serious efforts in the academic and policy communities to study how a nuclear war could end.[1] The large nuclear arsenals of the Americans and Soviets, the drift of US and Soviet military thinking, and the policy related anxieties of other skeptics, all precluded closure on this question before the Cold War ended. In a policy debate on the role of nuclear weapons polarized between the "deterrence only" and "actual use" schools of thought, the question of how to conduct a nuclear war controlled by policy and coherent strategy received short shrift.

The subject of nuclear war termination should be reopened now because the threat of nuclear danger has changed from one of quantity to one of quality – who has nuclear weapons, and for what purpose are they intended? The political and technological environments relevant to starting and stopping a nuclear war are markedly different from the Cold War context. It would be a major tragedy if in the aftermath of the first nuclear weapons fired in war since Nagasaki, neither the United States nor other great powers had thought through how to abort a nuclear conflict in its early stages. For unlike the hypothetical Armageddon between the Americans and Soviets that never occurred in the last century, smaller than global but nevertheless highly destructive nuclear wars could take place in this century. Some of these conflicts have the potential to spread into a wider war – for example, between India and Pakistan – that could engulf other nuclear powers in the Asia-Pacific region. Pakistan could find

Dr. Stephen J. Cimbala is a professor of political science at Pennsylvania State University.

itself supported by China, and India could find itself supported by Russia and/or the United States, initially by means of extended deterrence but later by actual conventional or nuclear strikes. In addition, although the likelihood of any deliberate nuclear attack by the US or NATO against Russia, or vice versa, is obviously small to nonexistent, the possibility of inadvertent nuclear war or escalation into nuclear first use in Europe is not to be excluded – including in Russia's declaratory military doctrine and in NATO contingency planning.[2]

This study will attempt neither to construct particular scenarios of war termination nor to examine important topics such as bargaining strategies or monitoring and verification of nuclear cease fires. The focus here is broader, namely, the political-military contexts for the management of nuclear crises and post-crisis force operations, including escalation control and war termination. Specifically, correcting the potential inability of states to terminate a nuclear war requires that military planners and policymakers first accept the concept of nuclear war termination as feasible and desirable. There are considerable obstacles standing in the way of that acceptance, not the least being the intellectual resistance by many, based on the assumption that deterrence is undermined by a willingness to plan seriously for its possible failure.

Deterrence: How Reliable?

The first use of a nuclear weapon by one state against another since 1945 will create a tectonic shift in the expectations of policymakers and military planners worldwide. The nuclear taboo that supposedly restrained the hands of crisis bound policymakers during the Cold War and for the remainder of the twentieth century will have been shattered. Left in its place will be uncertainty, and the plausible expectation that first use may be followed by retaliation and further escalation. Of course a nuclear power could choose to attack or coerce a non-nuclear state, primarily with conventional weapons but amplified by the shadow of its nuclear power. Such an attempt at coercion could incur condemnation from the international community and responses from allies of the victim, including those with nuclear weapons. North Korea's intermittent and unpredictable disputes with South Korea, including the sinking of a South Korean naval vessel in March 2010, illustrate political and conventional

military coercion supported by the tacit deterrence of North Korea's limited nuclear capability.

It is generally assumed that the possibility of a nuclear war is related in some unquantifiable but nonetheless discernible way to the number of states with nuclear weapons and to the amicability or hostility of the inter-state relations. Unfortunately for peace in the twenty-first century, the roster of states with nuclear arsenals is increasing. North Korea's official acknowledgment of its nuclear weapons capability has been followed by off-and-on international efforts through the six-party talks (the United States, Russia, China, Japan, South Korea, and North Korea) to negotiate a freeze, followed by a reversal of the DPRK's military nuclear program. These efforts have proved extremely frustrating for those negotiating with North Korea, and uncertainty about North Korea's intentions increased with the death of Supreme Leader Kim Jong-Il in January 2012 and his succession by his son, Kim Jong-Un, who sports a political and personal blank slate.

Along with North Korea's entry into the nuclear club, Iran is suspected of having a strong intent to weaponize its nuclear fuel cycle. The US and leading European Union states, including Britain, France, and Germany, have exerted diplomatic and economic pressure against Iran since 2004, attempting to persuade Tehran to stop short of a de facto or acknowledged nuclear weapons threshold capability. In addition, negotiations between Iran and the P5 (the permanent members of the UN Security Council: the United States, Russia, Britain, France, and China) and Germany seek to create an ongoing diplomatic engagement, supported by pressure on Iran from the International Atomic Energy Agency (IAEA) and the European Union to demonstrate additional transparency about its nuclear aspirations and infrastructure. Part of the problem for the P5+1 was to determine exactly with "whom" or what domestic factions they were negotiating: it appeared that alternative hard and soft views within Iran's political and military elites, including its Revolutionary Guards Corps and religious leadership, created a shifting kaleidoscope of Iranian intentions and negotiating positions.

Figure 1 summarizes expert estimates of the probabilities of various paths for Iran to nuclear explosive materials.

Figure 1. Probability Levels of Iranian Paths to Nuclear Explosive Materials

Method	Probability 2013	Probability 2014-15
Rapid jump at declared centrifuge sites to highly enriched uranium (HEU) using safeguarded LEU		
Natanz	low	low
Fordow	low-medium	low-medium
Rapid jump at undeclared, covert centrifuge site using the safeguarded LEU stockpile	low-medium	medium
HEU production under safeguards at declared centrifuge plants	low	medium
Parallel covert centrifuge program	low	medium
Secret production of HEU at declared safeguarded sites	low	low
Arak reactor and secret, undeclared reprocessing plant (reactor operational in 2014)	--	low
Laser enrichment to produce HEU	low	low
Illicit acquisition of fissile material overseas for use in nuclear weapons	low	low
Legal withdrawal from NPT followed by weapons production	low	low-medium

Sources: David Albright, Paul Brannan, Andrea Stricker, Christina Walrond, and Houston Wood, "Preventing Iran from Getting Nuclear Weapons: Constraining its Future Nuclear Options," Institute for Science and International Security, March 5, 2012, http://www.isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf, cited in Anthony H. Cordesman and Alexander Wilner, *Iran and the Gulf Military Balance – II: The Missile and Nuclear Dimensions*, Working Draft, Major Revision 5 (Washington, D.C.: Center for Strategic and International Studies, July 16, 2012), p. 40, www.csis.org/burke/reports. See also David E. Sanger and William J. Broad, "Iran Said to Nearly Finish Nuclear Enrichment Plant," *New York Times*, October 25, 2012, http://www.nytimes.com/2012/10/26/world/middleeast/iran-said-to-complete-nuclear enrichment-plant/html.

As of November 2012, neither diplomatic coercion nor various economic and political inducements led Iran or North Korea to nuclear abstinence.[3]

The existing state powers and international organizations had to decide what other steps short of war were available. One alternative was to put the matter of Iranian or North Korean nuclearization before the UN Security Council. Regarding this option, China was likely to block any serious sanctions against North Korea. Better prospects existed for multilateral (US and European) or international (Security Council) coercion of Iran. A series of UN resolutions since 2006 have increased pressure on Iran to comply with international arms control inspectors, to restrict its trade in nuclear and military related materials and equipment, to suspend enrichment and reprocessing activities, and to limit the activities of the Iranian Revolutionary Guards Corps (IRGC) and others suspected of engaging in prohibited activities. The European Union in January 2012 agreed on an oil embargo against Iran effective from July of that year and a freeze on the assets of Iran's Central Bank. In March 2012, Iranian banks in breach of UN sanctions were disconnected from SWIFT, a global coordinating hub for international financial transactions. A number of states have imposed bilateral sanctions against Iran, especially the US, with its almost total economic embargo and arms ban, including sanctions on Iranian financial institutions and companies doing business with Iran.[4]

Despite these and other sanctions, Iran's march toward the cusp of nuclear weapons capability appears inevitable, barring an unprecedented breakthrough in diplomacy or military action. A study by the Institute for Science and International Security has noted:

> If Iran is unwilling to make concessions to negotiate a long-term solution, the strategy must remain the alternative path of complicating and constraining Iran's pursuit of nuclear weapons capabilities or the weapons themselves. Achieving interim negotiated measures, such as caps on enrichment levels and centrifuge deployments, would remain important. But the main effort would entail a strengthened effort to delay, thwart, and deter Iran's pursuit of nuclear capabilities.[5]

The problem of containing proliferation among rogue or state actors was actually twofold. The first part was what to do with additional states having become nuclear capable. The second aspect was the valid concern that rogue nuclear powers might pass nuclear technology or know-how to non-state actors, including terrorists. It was known, for example, that even before 9/11 al-Qaeda had attempted to acquire nuclear weapons grade

material. The US and other countries with comparatively large national territories were ironically more vulnerable to some kinds of attacks by weapons of mass destruction (WMD), including chemical, biological, radiological, or nuclear weapons, in the sense that larger states have a greater variety of target sets to defend, including widely dispersed civilian infrastructure.

Some optimists about the probable consequence of further nuclear weapons proliferation among states might argue that deterrence would work in the future, as it presumably did during the Cold War. The optimism is based on the hindsight that we survived the Cold War without accidentally or deliberately setting off a US-Soviet nuclear exchange leading to a global catastrophe. Persons living through the Cold War and its various crises, especially the Cuban missile crisis, had a somewhat less deterministic view about the success of deterrence. Moreover, even if Cold War deterrence was as assured as optimists supposed, deterring terrorists and other non-state actors from nuclear adventurism is another task altogether.

Deterrence of non-state actors lies outside the scope of this essay, assuming that "deterrence" as a robust concept applies at all to prevention of terrorist attacks.[6] The objective of deterring rogue or other states is sufficiently challenging for Western planners and policymakers. Some government officials and others concerned about the behavior of rogue actors have concluded that they are in all likelihood beyond the grasp of rational deterrence strategies. At the very least, rogue actors might not be amenable to military persuasion by the US or any Western model of rational deterrence.

The US model of deterrence rationality emphasizes the cost-benefit calculations of various courses of action. Decision makers choose the alternative with the lowest anticipated cost and the largest potential benefit relative to other available alternatives. Deterrence theory is thus one aspect of public choice theory, and as such, it works only within a limited frame of reference or "bounded rationality." Within this framework, adversaries are assumed to have accurate information about one another's goals, alternatives, and positive or negative weights assigned to various options.

The vulnerabilities of this model of analysis, applied to the real world of nuclear crisis management, are serious and potentially deadly.[7] It is not so much that deterrence theory is more deficient in the abstract, compared to other possible approaches to conflict management. The challenge lies in

applying the abstract logic to a myriad of concrete situations. The specific circumstances of a crisis are important in understanding how it tumbled into a war. Once deterrence has presumably failed and war has broken out, the course of battle influences the remaining options for policymakers and commanders who wish to stop the war sooner rather than later.

It is a mistake to suppose that an outbreak of war is necessarily the result of deterrence failure. An adversary may be bent on attack come what may. Thus the motives and mindsets of possible enemies are as important as are their capabilities for determining whether and when they might attack. History is full of wars begun under assumptions about enemy intentions and capabilities that the test of battle later proved fallacious. Attackers have not infrequently begun wars against states with greater military capabilities. Often the attackers in question doubted the resolve of the defenders. In other instances, states misperceived one another's intentions relative to war because they failed to comprehend essential aspects of the other side's strategic culture, military planning priorities, or "art of war." Wars undertaken by leaders who err on one or more of these factors are sometimes referred to as "accidental" or "inadvertent" (usually by political scientists who favor these concepts, less often by historians who are more skeptical).

Deterrence during the Cold War, at least in US academic discourse and public policy analysis, was in constant danger of overstretch. For some analysts and policymakers it became a talisman that replaced hard data or serious thought. Deterrence was also sometimes substituted for policy instead of for military strategy (separate problems, but related). The domino theory that the US used to justify its military escalation in Vietnam is one example of deterrence (and its twin, credibility) stretched across the conceptual and geographical fault lines that separated war in Europe from war in Asia.

It would be premature to declare that aspiring nuclear powers, including rogue states, are "beyond deterrence" in the sense of existential deterrence. Nonetheless, deterrence will certainly operate differently in the twenty-first century compared to the Cold War. One reason for this is related to nuclear proliferation. Nuclear weapons were the hallmarks of great powers that during the Cold War were mostly content with the geopolitical status quo. Future nuclear aspiring or nuclear capable states, on the other hand, may be revisionists with regard to their international policy objectives.

In fact, the very term "rogue" or "state of concern" implies as much: the rogue is only roguish from the standpoint of those who favor the existing system and its parameters. Those who wish to overturn the system might regard rogues as heroes. In the eighteenth century, American and French revolutionaries were rogues against the established order: now their successor states are part of it.

Another question raised about deterrence is whether it can apply to heads of state, military leaders, or terrorists whose motives are apocalyptic or otherwise non-rational. This of course invites the question: what is a rational motive?[8] Suffice it to say that one state's rationality may be another's irrationality, but the distinction is not a clinical one. Individuals who are clinically suspect may nevertheless make clear decisions on behalf of their states in troubled times: indeed, many have done so. Rationality has to do with the logic of means and ends connections: is the state acting in a way that maximizes its likelihood of success in the event, or minimizes its probability of failure.

In a crisis between two nuclear powers, the difficulty rises because the decision logics or "rationalities" of the two sides are interdependent. Each has a sequence of moves that may be more or less logical, in reaction to the move of the other. This interdependency of moves and motives is what makes nuclear or other crises so hard to manage.[9] Imagine a two dimensional chess game with the players blindfolded, and with each side permitted a finite number of mistakes (say, two wrong moves) before the players and the board are blown to smithereens. The example is not fatuous: US President John F. Kennedy and Soviet Premier Nikita Khrushchev played something like this during the Cuban missile crisis.

Principles of Escalation Control

As related to the problem of ending a nuclear war, theories of escalation control contain several key propositions. All are controversial, but none is self evidently impossible. First, even nuclear war, however destructive, would involve political goals, at least at the outset. Second, states and leaders can be expected to recognize certain rules of the game about fighting and ending wars, despite cultural and national differences. Third, although time pressures and the military planning process impose constraints upon escalation control for war termination, success is not precluded in practice.[10] Paul Bracken has argued with reference to defensible Cold War

views of this matter: "The assumption of robustness with respect to time pressures and planning rigidities is supported by the certainty that in a nuclear crisis each nation's top leader would be at the helm, overriding bureaucratic obstacles of delay and omission."[11]

The idea of ending a nuclear war already in progress implies that deterrence can be applied to the problem of limiting a war as well as preventing it. A nuclear war is a failure of deterrence that has already happened. Worse, however, would be for the various parties to the conflict to continue firing until their arsenals were exhausted or all major cities destroyed. Getting combatants to the bargaining table after the shock of nuclear combat would not be easy. Unless the war was started by mistake, say an accidental launch or a rogue commander, important issues of state would be in dispute. In addition, the anger of survivors at the consequences of nuclear attacks on their society would be difficult for governments to manage. Survivors' demands for retaliation and revenge might overwhelm policymakers' efforts to arrange ceasefires or surrenders.

The termination of a nuclear war, as in any war, has both military-tactical and politico-strategic aspects.[12] The tactical situation on the battlefield is obviously important. After the early nuclear attacks have taken place, each side may have surviving forces. The surviving forces are bargaining assets that can be used in negotiating a ceasefire or peace agreement. Even a few surviving forces on either side can threaten to inflict a great deal of societal destruction on the other, and its leaders might prefer to negotiate instead of to continue fighting. However, in the chaos attendant to nuclear war, even a "small" regional war by Cold War standards, leaders and their military advisors might not have reliable information about the status of the enemy's forces and command and control systems.

Command and control systems present an anomaly to planners who might want to leave the door open for intra-war deterrence and nuclear war termination. On the one hand, in traditional military thinking based on experience in conventional war fighting, attacking command and control and communications systems makes perfect sense. It is an efficient way to destroy the opponent's military cohesion and coordination. Attacks on the enemy's brain and central nervous system, as were carried out during Operation Desert Storm, are important force multipliers that can be used to win a war in good time and save both friendly and enemy casualties.

But in a nuclear war, the destruction of enemy political or military command and control systems would almost certainly exacerbate the problem of ending the war, and at two levels. At the tactical level, the destruction of military control systems would cut the nuclear retaliatory forces and their commanders into separate pieces. Each piece would be programmed to continue firing and fighting unless otherwise directed to stand down. However, the stand down orders might never reach the relevant field commanders having custody of nuclear weapons, nor those authorized to fire them (who might be the same people, but not necessarily). Thus, "outliers" in the nuclear military chain of command might not hear, or want to hear, ceasefire orders.[13]

Destruction of the main political center of the opponent might paralyze its civilian leadership and make it impossible for the President or Prime Minister, or other surviving cabinet officials, to gain secure and reliable control over the armed forces.[14] Consider, for example, an Iranian attack on Israel, or a Pakistani strike against India, that "succeeded" in decapitating the heart of the enemy's political leadership. Effective control over the armed forces of the attacked states would almost certainly pass directly to the military and other security organs. The surviving political leadership in Tel Aviv and in India would at least temporarily be the prisoners of fast moving events and asserted military imperatives. It would take considerable time, and at least the appearance of an interim ceasefire, before anything like "normal" relationships between politicians and the armed forces were reestablished.

Assessment of the viability of command and control systems under the stress of nuclear or other WMD attacks is made difficult by the scarcity of reliable information in the public record. It might be supposed, for example, that each state or government has official, written arrangements for delegation of political office and for devolution of military command during crisis and war – across the spectrum of conventional and if necessary nuclear conflict. But this assumption could be mistaken for nuclear aspiring or new nuclear states. Even if written protocols exist, they may not be adhered to or correspond to reality once the shooting starts. In addition, the delegation of political authority and the devolution of military command and control may differ in important ways. Another uncertainty with respect to nuclear crisis or wartime command and control systems is how they might be affected by strategic or operational cyber war. For example, cyber

attacks preceding or accompanying kinetic attacks might make it more difficult to control military operations and to assess enemy intentions accurately, thereby confounding negotiation for war termination.[15]

The American Presidential Succession Act and various other legislative enactments, as well as Constitutional requirements, clarify both non-emergency and emergency procedures for answering the question "Who is in charge?" if the President is killed or disabled. The military chain of command, although it begins with the presidential center, is not identical to the political one. The wartime chain of military command proceeds from the President, to the Secretary of Defense, and then to the regional or functional combat commanders (through the Joint Chiefs of Staff). This system ensures that even if the political decision center is paralyzed by a surprise attack, the military commands authorized to retaliate can do so in a timely manner. These command and control arrangements were worked out over many years of Cold War trial and error. They were, and are, intended to provide a solution for the oxymoronic requirement that forces "never" be fired without appropriate authorization but "always" respond promptly when authorized missions are required.[16]

In the early years of the nuclear age, US policymakers and military leaders struggled to define a rule for the control of nuclear weapons in peacetime and for the management of nuclear forces during crisis and war. The Truman administration initially assigned custody over atomic weapons to a civilian agency. The weapons could only be released to the military by presidential order. As this became impracticable in the missile age, systems were required for dispersing weapons to the military while maintaining them in secure storage and proof against accidental or unauthorized use. In addition, land based, sea based, and air launched weapons required platform-specific protocols: aircraft could surge to "fail safe" points and wait for confirming orders before proceeding to attack. Missiles, on the other hand, are not subject to recall: their launch was an irrevocable decision for war.

Escalation Control: New Challenges

The details of US and Soviet Cold War force operations, including command and control, are not important here. Enough has been presented to stress that only over considerable time, and as a result of much trial and error on the part of operators and analysts, were these systems established

as reliable against usurpers or accidents and as responsive to authorized commands. The lessons learned by the Americans and post-Cold War Russians in this regard have not necessarily been passed along to future generations of nuclear capable states. The extent to which some existing nuclear powers, to say nothing of future ones, accept the idea of deterrence based on second strike capability, as opposed to preemption, is unclear. Nor are the relationships among the highest levels of political and military command, with regard to the alert of forces in crisis or the employment of forces in war, altogether clear for states such as Pakistan and North Korea. How custody of nuclear weapons along with the authority to fire them has been delegated to field commanders in India, Pakistan, Israel, or North Korea is a closely guarded secret.

Once nuclear weapons were fired in South or Northeast Asia or in the Middle East, would political leaders be able to maintain continued control over force employment, targeting, and termination decisions? States with small inventories of weapons, especially if they were first strike vulnerable, might follow the logic of "use them or lose them" and rapidly expend their existing arsenals. On the other hand, even smaller states might want to maintain some forces in reserve in order to avoid nuclear blackmail in the post-attack phase of a war. A small residue of survivable forces, perhaps tactical missiles or nuclear capable aircraft of limited range, could be the difference between an imposed surrender and a negotiated peace. Thus surviving but unexpended residual nuclear forces have two faces: they can be coupled to the credible threat of further escalation, or they can be attached to proposals for de-escalation and conflict termination. A war between nuclear armed states that continues until both or all combatants have totally exhausted their nuclear arsenals is a political failure, regardless of its military accomplishments. Such a war turns Clausewitz on his head and makes nuclear battle and mass destruction into pseudo-political ends in themselves.

In order for negotiations between India and Pakistan, or Israel and a nuclear Iran, to take place after the nuclear threshold has been crossed, leaders in firm control of their nuclear forces are a prerequisite. Leaders would have to survive the early attacks, communicate with their nuclear forces, and impose targeting restraints or even nuclear ceasefires. These steps to expedite negotiation might not be possible. Rogue commanders, once enabled to fire nuclear weapons, and having observed unprecedented

destruction on their own country, might resist ceasefires and become bent on revenge or holocaust. The delegation of nuclear release authority having been made from senior politicians and military commanders to force operators, retrenchment and "putting the genie back in the bottle" would call for wartime commanders to put professional obligations and the military chain of command ahead of personal agendas and motives. Some might, and some might not.

Nor is this problem one that has been entirely obviated among "mature" nuclear powers. Russia in the 1990s was in dire economic straits. As its economy lagged, its conventional military forces became cash starved and operationally deprived of oxygen. Consequently, Russia became primarily dependent upon its nuclear weapons, especially its long range weapons, for deterrence of major nuclear or conventional attacks on its state territory. Russia's position in the 1990s was like NATO's during the Cold War: presumed inferiority in conventional forces, and therefore an acknowledged reliance on nuclear weapons to project strength. In addition, after the fall of the Soviet Union, Russia's missile warning and control systems deteriorated, including its satellite and ground based radar networks. Russia's nuclear weapons complex and its nuclear scientific establishment were also casualties of its free falling economy. The US established programs of military assistance to Russia in the 1990s in order to improve Russia's handling of nuclear materials and weapons, including accurate accounting and safe storage and dismantlement.

This marks an ironic turn of events, compared to the Cold War: the US government is now a large "investor" in Russian nuclear safety and security. The concern in Washington is no longer the prospect of a deliberate Soviet nuclear attack, but of Russian loss of political or military control that leaves nuclear weapons and launchers in the hands of regional warlords. This subject is almost taboo in official diplomatic circles, but interestingly, the topic of Russian breakup or deconstruction into a plurality of regional entities is the subject of much speculation among Russians. Russian media and polling organizations frequently sample public opinion on this issue, and about a third of Russians generally regard the possibility of a breakup of post-Soviet Russia as more than trivial. The question in such an event is whether the split would be a case of gradual and consensual political devolution, or whether it would likely be associated with a civil war.

The current administration of President Vladimir Putin has made clear its intent to resist any regionalization or other dismemberment of Russia. Putin's firm opposition to Chechen terrorism and insurgency and Putin's absolute "nyet" to the demand for political autonomy or independence for that troubled region have been consistent and emphatic: there will be no departure from Russia by means of armed resistance. US policy is that Russia should indeed hold together, for a major breakup of Russia would destabilize the entire central Eurasian subcontinent with ripple effects to the west, east, and south. An immediate concern about a dissolving Russian polity would be the consequences for the command and control over its nuclear weapons and launch platforms.

The US and its allies have been in this situation once before. In the immediate aftermath of the Soviet breakup, the post-Soviet states of Ukraine, Belarus, and Kazakhstan were suddenly numbered among the world's nuclear powers. The fates of their respective nuclear arsenals were up for grabs, and various heads of state in these countries sought to play the nuclear card for economic assistance or for the temporary prestige it might bring them. US policy was to establish Russia as the logical and legal successor state to the Soviet Union for the purpose of controlling nuclear weapons and forces. Otherwise, dispersal of nuclear weapons among post-Soviet states could lead to chaos, including the unauthorized distribution of nuclear weapons and weapons grade materials among terrorists. After considerable political wheeling and dealing in the early 1990s that involved the US, Russia, and the new trio of nuclear powers, agreement was reached for the forces of Ukraine, Belarus, and Kazakhstan to be "returned" to Russia (standing in for the former Soviet Union) or dismantled.

Russia's nuclear weapons deployed for use on intercontinental missiles or long range bombers are, according to Russian officials, under secure storage and control in peacetime.[17] In the nearest approximation to a nuclear crisis during the 1990s, the launch of a Norwegian scientific rocket in January 1995 was temporarily confused by Russian warning systems with a possible US missile launch from a ballistic missile submarine. Russian nuclear forces were alerted. Russian President Boris Yeltsin, together with his Defense Minister and chief of the general staff, used – for the first time in the post-Cold War era – their nuclear "footballs" or briefcases that accompany the head of state and his principal military advisors. Russian tracking of the missile trajectory eventually established that its path was

headed out toward sea and away from Russian territory.[18] It turned out that the Black Brant missile launch that temporarily alarmed the Russians was the result of a diplomatic snafu. The Norwegian government had notified the Russian Foreign Ministry months in advance of the planned rocket launch and its purpose: gathering scientific data on aurora borealis. But the communication got lost in the Russian bureaucracy and never made it to the desks of the responsible officials in the Russian armed forces and Defense Ministry.

The preceding survey of concerns about mature nuclear powers is not intended to single out Russia, but to caution against casual acceptance of the assumption that "rogue" or new nuclear states would be more likely to start a war, and less willing to end a war short of Armageddon, than longstanding nuclear powers would be. Of course, the major powers' larger and more diverse arsenals give them options for controlling conflict and for intra-war deterrence, compared to smaller powers. And even at lower levels of force size, the qualities of forces and their operational parameters are partial determinants of their ability to maintain political and military control during a nuclear war.

That said, the decisions for prolonging or ending a war vary widely, based on the motives and personalities of leaders, as well as the moods of publics that were subject to attack. An additional variable for any state engaged in a nuclear war will be the policymaking process in that state: how power and influence are distributed among office holders and politically influential persons. We have some idea how the process of national security decision making works in the United States, Britain, France, China, and Russia, as these polities have been studied extensively by insiders and outsiders.

What power shifts, however, would take place after war began in India, Pakistan, North Korea, or Iran? North Korea is virtually opaque to foreign intelligence. Pakistan is a government under siege from jihadists whose influence extends into its military and intelligence organs. The regime in Tehran is torn between traditionalist ayatollahs with visceral hatred for the US and Israel and modernizers who would prefer to focus on economic development and gradual social change. India is the world's largest democracy and a remarkably stable one, but under the stress of a nuclear attack, the relationship between its military and its government might undergo drastic change, compared to its peacetime condition. Recall

that one Indian Prime Minister during the Cold War was assassinated by several of her own official bodyguards.

For that matter, what could we expect from an American President in the aftermath of a nuclear attack on US soil by a rogue or other, state? US history does not inspire confidence that cool heads would prevail and that the government would seek to manage a conflict toward "victory" at the lowest possible level of destruction or to negotiate an agreed peace. US reaction to 9/11 was instructive: not only terrorists everywhere, but regimes that aided terrorists, were placed into the crosshairs of American response. Al-Qaeda deserves all the opprobrium it received, but the point here is a different one. Americans and their political leaders are not, by temperament and training, accustomed to dealing out military punishment in measured doses. The likely reaction to a nuclear attack even by terrorists on US soil would be a public demand for a Carthaginian peace.

Conclusion

Nuclear war termination was controversial during the Cold War, and for different reasons it will continue to be so. Contemplation of the "awfulness" of nuclear war is certainly not to be expected of most politicians or publics, apart from the post 9/11 now-ubiquitous fears of nuclear terrorism. But apart from terrorism, states still have the responsibility for world order, and peacemaking does not stop after war has begun. Political leaders and military planners in nuclear armed and other leading states need to think through, before the fact of deterrence failure, what the "downstream" steps would be.[19] Military machines should not be permitted to run on nuclear autopilot.

The preceding illustrations do not constitute a prediction, but a template for considering some aspects of the problem of nuclear conflict termination. American and Russian forces were used for illustrations because we know something about how each state operated its nuclear forces during peacetime and in crises – and because they have committed themselves to structural and operational arms control through the year 2018. Finally, the diversity of US and Russian launch platforms, even at lower levels of force size, holds implications for smaller nuclear powers and for nuclear-aspiring, but currently non-nuclear states.

The management or prevention of nuclear proliferation is made harder by the uncertainty about relationships between politicians and

their militaries in countries that are only token democracies or less. How would arrangements for delegation of authority and nuclear enablement for deterrence or war fighting be handled in a nuclear armed Iran or Egypt or, for that matter, in currently nuclear capable North Korea and Pakistan? Opacity in these matters is not reassuring, and dictatorships have a way of appearing solid on the outside but brittle on the inside, once a diplomatic crisis has begun to slide into a war. In addition, future deterrence and war termination strategies will have to take into account the possible conjunction of weapons of mass destruction, including nuclear ones, with strategies for cyber conflict. It is a reasonable expectation that future interstate conflicts will include some measure of cyberwar; so too, will nuclear crisis management, escalation control, and conflict termination.[20]

Notes

1 See for example: Stephen J. Cimbala, ed., *Strategic War Termination* (New York: Praeger Publishers, 1986); Paul K. Davis, "A New Analytic Technique for the Study of Deterrence, Escalation Control and War Termination," in Stephen J. Cimbala, ed., *Artificial Intelligence and National Security* (Lexington, Mass.: Lexington Books, 1986), pp. 35-60; and George H. Quester, "War Termination and Nuclear Targeting Strategy," ch. 14, in Desmond Ball and Jeffrey Richelson, eds., *Strategic Nuclear Targeting* (Ithaca, NY: Cornell University Press, 1986), pp. 285-305. For a perspective on this issue at the end of the Cold War, see the essays in Stephen J. Cimbala and Sidney R. Waldman, eds., *Controlling and Ending Conflict: Issues before and after the Cold War* (Westport, Ct.: Greenwood Press, 1992).

2 "The Military Doctrine of the Russian Federation," www.Kremlin.ru, February 5, 2010, in *Johnson's Russia Lis*t 2010 - #35, February 19, 2010, davidjohnson@starpower.net. See also Nikolai Sokov, "The New, 2010 Russian Military Doctrine: The Nuclear Angle," Center for Nonproliferation Studies, Monterey Institute of International Studies, February 5, 2010, http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm; and Jacob W. Kipp, "Russia's Nuclear Posture and the Threat that Dare Not Speak its Name," ch. 10, in Stephen J. Blank, ed., *Russian Nuclear Weapons: Past, Present, and Future* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2011), pp. 459-503.

3 The cases of North Korea and Iran may require different treatment from the perspectives of deterrence and nonproliferation because North Korea is a declared nuclear weapons state and Iran is still an allegedly aspirational one. See Amitai Etzioni, *Security First: For a Muscular, Moral Foreign Policy* (New Haven, Yale University Press, 2007), pp. 241-42.

4 For a history of Iran's nuclear program, including a documented list of Iran's violations of its Safeguards Agreement with the International Atomic Energy Agency, see Iran Watch, "Iran's Nuclear Program, " updated March 2012, http://www.iranwatch.org/wmd/wmd-nuclear essay-footnotes.htm, downloaded August 13, 2012. See also "Sanctions against Iran," *Wikipedia*, http://en.wikipedia.org/wiki/Sanctions_against_Iran.

5 David Albright, Paul Brannan, Andrea Stricker, Christina Walrond and Houston Wood, "Preventing Iran from Getting Nuclear Weapons: Constraining its Future Nuclear Options," Institute for Science and International Security, March 5, 2012, p. 45, http://www.isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf. Albright et al, also outline elements of a five stage framework agreement between the P-5+1 and Iran, pp. 42-44.

6 For informative discussions of nuclear terrorism, see: Brian Michael Jenkins, *Will Terrorists Go Nuclear*? (New York: Prometheus Books, 2008); Etzioni, *Security First*:, esp. pp. 218-43; and Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books − Henry Holt, 2004). For additional perspectives on nuclear terrorism, see Morten Bremer Maerli, Annette Schaper, and Frank Barnaby, "The Characteristics of Nuclear Terrorist Weapons," pp. 209-22; Matthew Bunn and Anthony Wier, "The Seven Myths of Nuclear Terrorism," pp. 223-35, and John Mueller, "The Atomic Terrorist?" pp. 236-54, all in James J. F. Forest and Russell D. Howard, eds., *Weapons of Mass Destruction and Terrorism*, 2nd ed. (New York: McGraw-Hill, 2012).

7 For pertinent critiques of deterrence theory as applied to post-Cold War issues, see Colin S. Gray, *The Second Nuclear Age* (Boulder, Colo.: Lynne Rienner Publishers, 1999), esp. pp. 88-93; and Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington, Ky: University Press of Kentucky, 1996. See also Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003), pp. 238-84.

8 On the issue of rationality and deterrence, see Morgan, *Deterrence Now*, pp. 42-79.

9 The work of Thomas Schelling on this topic as applied to nuclear deterrence is seminal, as in *Arms and Influence* (New Haven: Yale University Press, 1967). See also Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave-Macmillan, 2003), esp. pp. 171-84.

10 Paul Bracken, "War Termination," ch. 6, in Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds, *Managing Nuclear Operations* (Washington, D.C.: Brookings Institution, 1987), pp. 197-214.

11 Ibid., p. 201.

12 Bracken, "Delegation of Nuclear Command Authority," ch. 10, in *Managing Nuclear Operations*, pp. 352-72, esp. pp. 355ff., offers similar if slightly different distinctions between "provincial" and "political" control. Provincial

control includes strategic and tactical control of the armed forces; political control deals with grand strategy, which is essentially policy.

13 Various aspects of this issue are discussed in Bracken, *The Command and Control of Nuclear Forces* (New Haven, Ct.: Yale University Press, 1983).

14 Perspectives on this and related problems appear in Albert Wohlstetter and Richard Brody, "Continuing Control as a Requirement for Deterring," ch. 5, in Carter, Steinbruner, and Zraket, eds, *Managing Nuclear Operations*, pp. 142-96. See also Bracken, "Delegation of Nuclear Command Authority," p. 359. As Bracken observes, delegation of nuclear command authority by political leaders to others will not happen except in the most dire circumstances – which are exactly those in which a nuclear war will most likely take place (Ibid., p. 356).

15 Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense," *Joint Force Quarterly* 61, no. 2 (2011): 18-23, esp. p. 21 on escalation control of "I2Os" (information and infrastructure operations). See also U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, July 2011), http://www.defense.gov/news/d20110714cyber.pdf, downloaded August 14, 2012, and The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: The White House, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. For pertinent commentary on these documents and related issues, see Rosemary M. Carter, Brent Frick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Force Quarterly* 66, no. 3 (2012): 22-27.

16 This perspective is developed in Peter Douglas Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, NY: Cornell University Press, 1992), pp. 12-28. See also, in the same volume, his comments on civilian control after the decision to use nuclear weapons, pp. 55-66.

17 Weapons grade or other nuclear materials, including vast stores of uranium and plutonium, are another matter. US and other nonproliferation experts remain concerned about leakage from Russia's nuclear weapons complex or other sources of nuclear or radiological materials. This is a separate, albeit important, subject. See Andrew and Leslie Cockburn, *One Point Safe* (New York: Doubleday, 1997), for pertinent cases and arguments based on Russian post-Cold War experience in the 1990s.

18 Ibid., pp. 240-44.

19 An excellent case is made for this point in George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore, Md.: Johns Hopkins University Press, 2006), esp. pp. 24-52 and 90-126.

20 For an appreciation of cyber war in strategic context, see Colin S. Gray, "Making Strategic Sense of Cyberpower: Why the Sky is Not Falling," paper, Wokingham, Berkshire, UK, September, 2012, esp. pp. 7-9.

Israel's Second Lebanon War Reconsidered

Benjamin S. Lambeth

Operation Change of Direction, the code name given to Israel's war against Hizbollah in Lebanon in 2006 by the Operations Directorate of the Israel Defense Forces (IDF), was the most inconclusive performance by far in the IDF's many trials by fire since 1948, in that it represented the first time that a major regional confrontation ended without a clear cut victory on Israel's part. The campaign's uneven course and outcome did not emanate from any particular single point failure but rather, in the words of two informed commentators, from "an overall accumulation of circumstances."[1] More specifically, it did not reflect any failure of Israel's well endowed air arm to perform to the fullest extent of its considerable but not unlimited capabilities, as many were quick to complain.[2] Rather, it resulted from a more overarching deficiency in strategy choice, whose most flawed elements were inconsistency between avowed goals and the available means and will to pursue them, and the Israeli government's initial placement of friendly casualty avoidance above mission accomplishment in its ranking of campaign priorities.[3]

What mostly accounted for the frustration felt throughout Israel as the conflict unfolded was the fact that at no time during the 34 days of combat were IDF forces able to stem the relentless daily barrage of short range Katyusha rockets that Hizbollah fired into civilian population centers in northern Israel until a mutually agreed ceasefire put an end to that deadly harassment. Beyond that, the war's achievements fell short of what Prime

Dr. Benjamin S. Lambeth is a Senior Fellow at the Center for Strategic and Budgetary Assessments in Washington, D.C. This article is largely based on his *Air Operations in Israel's War against Hezbollah: Learning from Lebanon and Getting It Right in Gaza* (Santa Monica, CA: RAND Corporation, 2011). The full study is available at http://www.rand.org/pubs/monographs/MG835.html.

Minister Ehud Olmert had promised the Israeli people at the campaign's outset, namely, an unconditional return of the two IDF soldiers that Hizbollah abducted on July 12, 2006, which triggered the counteroffensive in the first place, and a decisive elimination of Hizbollah's military presence in southern Lebanon.[4] Not only did the IDF's lackluster performance adversely affect the longstanding image of Israel's invincibility in the eyes of the Arab world and the West; it reflected manifold failures in objective setting and expectations management at the highest levels of the Israeli government, both uniformed and civilian.[5]

It would be wrong, however, to suggest from this generally accepted overall view of Israel's Second Lebanon War, as one American did a year after the fighting ended, that playing up its accomplishments, of which there were many, "is a little like saying that the operation was successful but the patient died."[6] On a more positive note, the IDF Chief of Staff who oversaw the planning and conduct of the campaign, Lieutenant General Dan Haloutz, who rose the ranks through the Israel Air Force (IAF), remarked presciently during his subsequent testimony to the Winograd Commission that assessed the IDF's performance that "whatever was or was not achieved [during the campaign] must be judged in the perspective of time."[7] Prime Minister Olmert likewise suggested in his testimony to the commission that "the results of the [war] will look better with time."[8] Consistent with these more upbeat early official judgments, the campaign experience has gradually come to be seen differently in Israel today than it was when the smoke of battle was cleared in August 2006. As early as 2008, a new debate began gathering momentum among Israelis over "whether or not we actually lost the war."[9]

Why the War was not a Total Loss for Israel

It was easy enough for Hizbollah commander and leader Hassan Nasrallah to claim in the campaign's early aftermath that he had "prevailed" simply by virtue of having survived. Yet the fact is that as a result of the IDF's counteroffensive, the Hizbollah organization suffered significant setbacks and paid a high price for its provocation on July 12, 2006 that was the casus belli for the campaign. The IDF killed nearly 700 of its most seasoned combatants and wounded more than a thousand.[10] In addition, a considerable portion of Hizbollah's military infrastructure in Lebanon

was either laid waste or badly damaged as a result of the IDF's relentless aerial and artillery bombardment.[11]

To note only the most important of the IDF's other achievements in this respect, the majority of Hizbollah's long range Zelzal and medium range Fajr rockets were destroyed during the campaign's first night by a well planned and practiced preemptive attack by the IAF, a largely unheralded first in the annals of air warfare. Nasrallah's command and control nexus in the Dahiye section of Beirut was also all but completely destroyed by precision IAF strikes.[12] Furthermore, Hizbollah's multiple barrel rocket launchers were repeatedly attacked and destroyed by the IAF within just minutes after their launch crews had fired their first round into northern Israel. The IAF's unprecedented rate of success in these time-sensitive targeting attacks could well have an inhibiting influence on any future indiscriminate use of such launchers by Hizbollah, and could drive its combatants to resort instead even more to single barrel launchers that can fire only one rocket at a time before being moved out of harm's way and reloaded.[13]

In addition, despite Nasrallah's continuing claim to have won a "divine victory" in the Second Lebanon War, Hizbollah's threat potential was severely diminished by the IDF's unexpectedly massive counteroffensive. As IAF Major General (ret.) Isaac Ben-Israel rightly noted in this regard, Operation Change of Direction "overturned the notion that Israel is not ready to fight with anyone who holds a sword over the heads of its civilians." In addition, he pointed out, "the destruction of a section of an Arab capital city, even a section that was directly associated with Hizbollah's main headquarters in Lebanon, set a precedent that should make Israel's enemies think twice the next time."[14]

The campaign also made for an instructive experience for the IDF in that it unmasked the true nature of Hizbollah as an enemy, its strengths and weaknesses, how it fights, and the lethality of its Iran-supplied rockets and anti-tank weapons. Moreover, in undertaking its response with such sustained intensity, Israel showed its determination to deal with Hizbollah using grossly disproportionate measures should a future challenge be deemed to require such *force majeure*. Israeli military historian Martin Van Creveld pointed out in this regard that "if anybody had predicted, a few days before the war, that in response to the capture of two of its soldiers, Israel would launch an air campaign over all of Lebanon, mobilize three of

its divisions and send them across the border, and keep up the pressure for over a month while taking thousands of rockets and suffering more than a hundred casualties in dead alone, he would have been considered stark raving mad." In all, added Van Creveld, in light of that response and the implied promise of more like it should Israel again be similarly provoked, "Nasrallah has good reason to think twice before engaging in another adventure of the same kind."[15]

In sum, the IDF's 34-day counteroffensive against Hizbollah was not quite the unqualified setback for Israel that many initially thought. Consider, in this regard, the post-campaign reality that Operation Change of Direction occasioned for both Hizbollah and Israel. From the very first weeks of his selection as Hizbollah's commander in 1992, Nasrallah had regularly, and with impunity, lobbed short range rockets into northern Israel until the start of the Second Lebanon War. Yet not a single rocket was fired from Lebanon into Israel during the years since the campaign ended until three rockets were launched during the IDF's subsequent 23-day operation against Hamas in the Gaza Strip in December 2008 and January 2009. Even though Hizbollah by that time had accumulated more short range rockets (as many as 40,000) in its since-reconstituted weapons inventory than ever before, its leaders were quick to disavow any responsibility for those launches.[16] Since then, the Lebanese border region has remained quiescent, indicating that Israel's deterrent against Hizbollah has held firm.

Nasrallah's Changed Risk Calculus

This new and so far persistent reality on Israel's northern border suggests that Nasrallah's post-campaign motivations and conduct were most definitely affected by the significant blow that the IDF dealt to his organization. He almost surely has been successfully intimidated by the lesson taught him by the IDF from any further gratuitous firings of rockets into northern Israel, a lesson that was doubtless reinforced by Israel's equally punishing subsequent campaign against Hamas two years later. Moreover, as a result of his awareness that he remains targeted by the IDF, Nasrallah and his main deputies have been forced to command from their bunkers and, with but few exceptions, have not appeared in public since the Second Lebanon War ended.

In this regard, commenting on a highly publicized "victory parade" that Nasrallah staged in Beirut in mid September 2006 about a month after the fighting in Lebanon ended, a senior source close to Prime Minister Olmert said: "Nasrallah doesn't look good. He looks exactly like someone who has been spending his time in a bunker, far from the sun, since July 12."[17] This source further noted that on the eve of Nasrallah's much-ballyhooed event, the Israeli security establishment debated whether to seize the opportunity to go after him even at the potential cost of causing hundreds of casualties among the surrounding Lebanese civilians. In the end, the government chose not to proceed with an assassination operation after senior leaders concluded that such an attack, at the likely price of many fatalities among innocent Lebanese, would have done Israel more harm than good. However, added the Israeli source, "The man will spend many more years in the bunker. He's a dead man."[18] Before the 2006 war, it was Nasrallah's practice to participate in more than a dozen highly publicized events each month. For one whose impact as a charismatic leader has long depended so heavily on frequent public exposure, his having since been forced to command from hiding has made for a major blow to his former effectiveness.

Furthermore, Israel inherited a significantly improved situation in southern Lebanon as a result of the campaign experience. On August 11, 2006, with the final countdown to an escalated IDF ground offensive rapidly nearing, the United Nations Security Council unanimously approved Resolution 1701, which called for a halt to the fighting and authorized the deployment of 15,000 foreign troops to the war zone to help the Lebanese army take control of southern Lebanon. The resolution, which was approved soon thereafter by the Israeli and Lebanese governments, further allowed the UN to take "all necessary action" to ensure that areas in which its forces would be patrolling were "not utilized for hostile activities of any kind."[19] It also called for the disarmament of Hizbollah's forces in southern Lebanon and the establishment of an enlarged United Nations Interim Force in Lebanon (UNIFIL). To help further enforce a semblance of order in the conflicted region, the Lebanese army began deploying in southern Lebanon on August 17, 2006.

To be sure, both the Lebanese government and UNIFIL subsequently retreated from their initial avowed commitment to disarm Hizbollah, and the presence of Lebanese army troops in southern Lebanon has

done nothing to curtail Hizbollah's continued fighting potential opposite northern Israel. Offsetting those all but predictable disappointments, however, has been the abiding fact that Nasrallah was plainly chastened by the IDF's unexpected response to his abduction of the two Israeli soldiers in July 2006 and has bent every effort to keep the border area calm so as to prevent a replay of the IDF's disproportionate counteroffensive. As a senior IDF commander observed within just a week after the campaign ended, "This is the huge change [that] this operation created."[20] Another commentator similarly noted a year later that "the last few months have been the quietest period on the northern border since Operation Peace for Galilee in June 1982." He further noted that "focusing the public debate [solely] on the failure in the Second Lebanon War and ignoring its achievements entirely may [adversely] influence the IDF's ability to learn from experience and draw the proper conclusions."[21]

Indeed, in reflecting on the various elements of guarded good news for Israel as a result of the campaign's outcome, a retired Israeli intelligence officer concluded that although the Second Lebanon War failed to diminish Hizbollah's long term threat potential or produce a significant change in the nature of Israel's standoff against the terrorist organization, it yielded four distinct positive achievements. First, it provided timely insights into Hizbollah's most advanced combat capabilities. Second, it helped reduce anxieties regarding what actions Iranian proxies like Hizbollah might take against Western interests. Third, it gave Israel an early look at what it will need to do to retool its capabilities for its next confrontation with Hizbollah. And last, it gave Israel's politicians an incentive to rethink the wisdom of their policy of giving up land for peace, as they did in Gaza and in parts of the West Bank in 2005.[22]

Looking back over the campaign experience, one can further ask whether Nasrallah, in planning his abduction gambit, fundamentally misread Israel's fortitude by so grossly underestimating the likely intensity of the IDF's response. Even as the Israeli counteroffensive was still under way, the deputy chief of Hizbollah's political arm, Mahmoud Komati, told Western reporters that he had been surprised by the force of the Israeli reaction and that Hizbollah's leaders had anticipated only "the usual, limited" reprisal by the IDF, such as commando raids or limited air attacks.[23] For his part, shortly after the ceasefire went into effect, Nasrallah himself frankly admitted that he would never have ordered the capture of

the IDF soldiers had he known beforehand what would follow by way of an IDF response: "You ask me if I had known on July 11…that the operation would lead to such a war, would I do it? I say no, absolutely not."[24] Toward the end of the campaign's second week, as the IDF's response was just moving into high gear, the American columnist Thomas Friedman, against the grain of the still-fashionable belief in many quarters that Nasrallah was the most "brilliant" and "strategic" Arab player, offered perhaps a more accurate assessment that "when the smoke clears, Nasrallah will be remembered as the most foolhardy Arab leader since Egypt's Gamal Abdel Nasser miscalculated his way into the Six Day War."[25]

That latter assessment can claim considerable strength from the premature frittering away of much of Iran's long term investment in Hizbollah that Nasrallah's headstrong provocation in 2006 occasioned. Indeed, Iran's provision of rockets of all types to Hizbollah could arguably be compared in overarching intent to the Soviet Union's forward deployment of medium range ballistic missiles to the Western hemisphere that culminated in the Cuban missile crisis of 1962, with the IDF having finally implemented measures analogous to those of the United States in dealing with the challenge militarily. As one informed Israeli observer noted in this regard, Iran built up Hizbollah's well stocked inventory of rockets with the idea that the latter would constitute, in effect, a "forward aircraft carrier" stationed close to Israel's border. In his judgment, this capability "was supposed to remain concealed until the moment of truth – a military conflict between Israel or the United States and Iran over Iran's nuclear weapons program. Their premature discovery, in light of the terrible blow they could have struck [against Israel], caused a strategic loss for Hizbollah and for its Iranian suppliers that cannot be denied."[26]

As if to bear that judgment out, the Iranian National Security Council, according to one report, received an internal document not long after the fighting ended indicating deep irritation over Hizbollah's "waste of Iran's most important military investment in Lebanon merely for the sake of a conflict with Israel over two kidnapped soldiers."[27] Such a reaction by Iran's ruling mullahs would not be surprising, considering that IDF operations during the 34-day war essentially wiped out much of the $4-6 billion that the Iranian treasury had sunk into building up Hizbollah's military strength, thereby necessitating a costly emergency Iranian outlay to reconstitute Hizbollah's military infrastructure and weapons stocks.

A New Strategic Chessboard for Israel

In all events, Hizbollah's role as a forward combat arm of Iran was starkly dramatized by the campaign experience, thus bringing into ever sharper focus the IDF's already considerable appreciation of the seriousness of the Iranian threat and giving its leaders an enhanced understanding of the threat that they also faced from Hamas. In addition, Hizbollah's image as a would-be guardian of Lebanese interests was badly tarnished by the costly consequences of Nasrallah's provocation for Lebanon's economy and civilian infrastructure. The terrorist leader now has a new understanding of the Israeli mindset and of the actual extent of what he can and cannot get away with in the future. Thanks to the scale and extent of its response, Israel demonstrated to Hizbollah that it is prepared to pay a high price in effectively retaliating against future tests of its resolve. The experience also spotlighted serious readiness problems in the IDF's ground forces and significant deficiencies in both air-ground integration and the provision of close air support to engaged ground troops by the IAF. Both problems have since been rectified, as was well attested by the IDF's more effective subsequent combat performance against Hamas in December 2008 and January 2009.[28]

Moreover, at the strategic level, Israel's experience during the Second Lebanon War drove home the emergent reality that a non-state adversary of Hizbollah's relatively sophisticated armament and orientation was far more than just a nuisance factor in the nation's security planning. On the contrary, with its revealed ability to hold large numbers of Israeli civilians at risk with its rocket inventory, the radical Islamist movement had in fact become what one Israeli analyst aptly described as "a strategic threat of the first order."[29] As two Australian scholars later commented, the proliferation of such cheap but effective terror weapons throughout the region had the almost instant effect of undermining "the historical importance of air power as the main instrument of Israel's deterrence policy."[30]

In a related vein, American defense analyst Andrew Krepinevich well characterized the Second Lebanon War as "the proverbial canary in the coal mine" in the way in which it spotlighted how "a new, more deadly form of irregular conflict …under high-technology conditions" had underscored the increasingly pronounced difficulty of defending major military installations, economic infrastructure, and densely populated rear areas against hybrid opponents like Hizbollah and Hamas armed with what he

called RAMM (rocket, artillery, mortar, and missile) capabilities.[31] Clearly concluding from its fresh memories of Lebanon that standoff-only attacks could not offer an adequate answer to this new challenge, the IDF got it right the next time around, in Gaza, by applying its emergent realization that the only way of dealing with such RAMM threats decisively was by "taking control of enemy launching areas....Thus, [in Gaza], Israel once again [came] to rely on a large maneuvering force, and the principle of waging battle on enemy territory [returned]."[32] Yet another reason why the IDF performed better in Operation Cast Lead in Gaza than it did during the Second Lebanon War was that this time its leadership and the Olmert government were willing, if need be, to sustain troop losses, which in the end proved to be far less than anticipated.

In all of the above respects, said one Israeli commentator, "it is almost as if Israel should thank Hizbollah for the wake-up call."[33] A big part of that wake-up call was a dawning realization that in fighting Hizbollah, the IDF was actually engaging a forward combat arm of Iran. Said one Israeli: "A huge, dark, perpetual forest of Katyushas is blooming in front of us. It is the State of Israel's tremendous good fortune that it is happening now and not later." This commentator added: "Nasrallah has lost the ability to deter us. He said that what goes for Beirut goes for Tel Aviv, and before he even finished talking we leveled another ten buildings in Beirut. He understands we are no longer afraid of him – no longer frozen.... He's the one who's [now] in an existential battle."[34]

In light of the major setback that the IDF counteroffensive during the Second Lebanon War dealt both to Hizbollah as a terrorist organization and to Iran's strategic interests, to say nothing of the uninterrupted calm that has prevailed along Israel's northern border ever since the ceasefire went into effect in August 2006, one can safely say in hindsight about Operation Change of Direction what the American essayist Mark Twain once supposedly said about Wagnerian opera – it's not as bad as it sounds. Viewed in hindsight, the three main strategic goals that General Haloutz declared for the IDF – stopping terrorist attacks by Hizbollah into Israel from sovereign Lebanese soil, making the Lebanese government responsible for policing its southern region, and inflicting significant damage on Hizbollah's military infrastructure – were all achieved in the end.[35] The only significant remaining downside, as IAF Brigadier General Itai Brun frankly admitted in a reflection on the campaign experience, is

that "we [the IDF and the Olmert government] failed to protect Israel's civilian population and did not succeed in shortening the war."[36]

To be sure, thanks to Iran's and Syria's continuing financial largesse and technical support, Hizbollah and Hamas are now assessed as having accumulated a combined inventory of as many as 70,000 short-range rockets.[37] Moreover, according to information reportedly acquired by Israeli intelligence and subsequently leaked to the press by Israel's President, Shimon Peres, Syria also has provided Hizbollah with a shipment of Scud-B missiles that possess the range and payload capability to hit any city in Israel with a 2,000-pound warhead.[38] If that report is correct, the transfer of Scuds to Nasrallah would make his organization the first non-state entity to possess such highly destructive (if unguided and inaccurate) surface-to-surface weapons.

On the negative side, however, Hizbollah has experienced a surfeit of highly publicized setbacks. For example, on July 14, 2009, an explosion destroyed a major ammunition dump maintained by the terrorist organization in the southern Lebanese village of Hirbet Salim. The following October, another secret munitions bunker maintained by Hizbollah in southern Lebanon blew up under obscure circumstances. Both events caused Hizbollah perceptible discomfiture by revealing the organization to be in violation of UN Security Council Resolution 1701 that prohibits the stockpiling of weapons south of the Litani River. To make matters worse for the organization's public image, Hizbollah combatants, aided and abetted by Lebanese army troops, prevented foreign inspectors from examining the site of the latter incident, thereby exposing the Lebanese army's lack of neutrality and its provision of active aid and support to Hizbollah.[39]

On top of that, more than a year before, on February 12, 2008, Hizbollah's military commander and Nasrallah's single most valued deputy, Imad Mughniyeh, was killed in Damascus by a mysterious car bomb explosion. At the terrorist mastermind's funeral in Beirut the following day, Nasrallah blamed Israel for having assassinated his right hand man and swore that Hizbollah's retribution would not be long in coming.[40] To this day, however, Nasrallah has not exacted his promised revenge for this devastating blow that was dealt to his organization's fighting edge.[41] (Among numerous other acts of notoriety, Mughniyeh was strongly suspected of having planned and overseen the July 12, 2006 border provocation that set off the Second Lebanon War.[42])

In addition, Hizbollah has been a lightning rod for gradually mounting Lebanese popular discontentment since the end of the IDF counteroffensive in 2006 as the main instigator of Israel's retaliatory bombardment that generated such widespread damage to Lebanon's civilian infrastructure and economy. For that reason, Nasrallah fully appreciates that he cannot afford to be viewed by the Lebanese rank and file as the cause of yet another painful Israeli retaliation against Lebanon. Also for that reason, only at the greatest risk to Hizbollah's own interests as an infectious presence within its Lebanese host can he commit any future act of aggression against Israel sufficiently grave as to precipitate an even more massive response of that sort by the IDF.

Looking Forward from Israel's Second Gaza Conflict

Israel's intelligence monitoring of Hizbollah is said to be greatly improved over what it was before the Second Lebanon War, and the IDF Northern Command has voiced confidence that the indecisive outcome of Operation Change of Direction in 2006 will not be repeated in case of another showdown with Hizbollah. Said one of its senior officers in October 2009: "By all means let Hizbollah try. The welcome party that we are preparing for them [this time] is one that they will remember for a very long time."[43] In addition, Israel's current leadership has left no room for doubt that because Hizbollah has inserted itself even further into the formal structure of the Lebanese government, any future act of aggression by the terrorist organization would be deemed an act undertaken by that government, thereby rendering Lebanon's infrastructure and economy legitimate targets for IDF retaliation.

Furthermore, with Hizbollah's hard line sponsors in Tehran now facing mounting troubles of their own given the slowly simmering discontentment on the home front, Nasrallah can no longer, at least for now, count on the automatic support of Iran in case of another Israeli assault on his most valued assets in Lebanon. "In short," in the words of a well-informed Israeli defense reporter, "despite the fact that Hizbollah today is substantially stronger in purely military terms than it was [in 2006], its political stature and autonomy have been significantly reduced. It is clear that Nasrallah is cautious, and he will weigh his options very carefully before embarking on any course of action that might lead to all-out war with Israel."[44]

In addition, in large measure due to the manifold incentive generated by Israel's having suffered two successive rocket wars in a span of less than three years, compounded by the continuing possibility of worse challenges yet to come from Hizbollah and Hamas, Israel's research and development establishment made major strides after 2006 toward fielding a serviceable active defense against the Grads, Katyushas, Qassams, and other short range rockets that plagued the IDF and the Israeli civilian population during the Second Lebanon War and in the months that preceded Operation Cast Lead in Gaza. In addition to its Arrow 2 and Arrow 3 area-defense anti-missile systems against long range ballistic threats and to its David's Sling interceptor aimed at destroying medium range rockets and slower flying cruise missiles, the IDF in 2010 began deploying its Iron Dome point defense system against short range rockets of the sort fielded in large numbers by Hizbollah and Hamas.

Until late 2012, the IDF's mobile Iron Dome interceptors were mainly positioned around Israeli towns and facilities closest to the Gaza Strip, as that Hamas-occupied bastion was the sole source of periodic rocket fire into populated areas of Israel after Operation Cast Lead ended in January 2009. Eventually, however, a total of 13 Iron Dome batteries will be fielded at strategically significant locations throughout Israel. The aim is to negate, ultimately decisively, the attack tactic currently most favored by Hizbollah and Hamas, i.e., firing short range, high trajectory unguided rockets into Israel's population centers for their terrorizing effect. Partly financed by the United States and incorporating advanced American radar and other technology, the Iron Dome system has not proven effective against mortars. Moreover, some have voiced concern that militant groups like Hizbollah and Hamas could attempt to overwhelm the system by unleashing heavy barrages of cheap short range rockets, thereby forcing the IDF to spend as much as $50,000 a shot to negate them. However, as an IDF spokesman commented in this regard, "there is a bigger issue here than how much it costs. [The Iron Dome system] is going to give us some answers."[45]

Earlier in 2012, such answers seemed to be coming increasingly into hand, in light of Iron Dome's successful interception in tests of a number of rockets that mimicked the scores of thousands of Qassams and Katyushas in the Hizbollah and Hamas arsenals. In those tests, the system used radar that acquires the incoming rocket and guides a kinetic interceptor to engage and negate it. The radar further succeeded in detecting rockets that were

headed toward predicted impact points known to be in uninhabited areas, thereby allowing the interceptor rocket to be withheld so as not to waste it against a nonthreatening target.[46] In March 2012, the targeted killing of a senior member of the Palestinian Popular Resistance Committees by an IAF air strike prompted a renewed barrage of Qassams out of Gaza, with some 250 launched into southern Israel as of the end of that month. By then the operational Iron Dome system intercepted nearly 90 percent of rockets that threatened to land in a vital area.[47]

This encouraging early showing of Iron Dome in its first combat test was reconfirmed on a larger and more definitive scale eight months later during the IDF's eight-day air offensive against Hamas, Operation Pillar of Defense, conducted in November 2012. That offensive was unleashed in response to a steadily escalating resumption of rocket fire by Hamas into southern Israel in previous months that was prompted by the encouragement its leaders perceived as empowering developments occasioned by the so-called "Arab Spring" in Egypt and elsewhere in the Islamist world.[48] In a masterful opening retaliatory strike enabled by precise real-time actionable intelligence, the IAF succeeded in killing Hamas's military commander, Ahmed al-Jabari, by means of an accurate air attack while he was riding in a moving vehicle. Over the course of the operation's eight days, the IAF also systematically obliterated all known and geolocated Hamas rocket storage sites, command and control facilities, and other vital military equities throughout the Gaza Strip.

This time, in marked contrast to its earlier experiences in Lebanon in 2006 and in Gaza in 2008 and 2009, the Israeli government took special care to ensure that overarching political goals and diplomatic efforts aimed at achieving them would be the main determinants of IDF combat actions. Treating its latest counteroffensive against Hamas as more an armed negotiation than a full-fledged war, the administration of Prime Minister Benjamin Netanyahu, with the crucial assistance of Egypt's democratically elected President Mohamed Morsi, consciously strove throughout for a negotiated ceasefire that might provide a more durable halt to Hamas's rocket fire into Israel in return for a gradual easing of Israel's blockade of the Gaza Strip aimed at hindering the influx of covert weapons shipments to Hamas by Iran and Syria through the Sinai Peninsula. The ceasefire was pursued by the Israeli government from the very start in conscious awareness that in order to achieve its desired political goals, the price it

would have to pay would be the avoidance of a major decisive combat operation against Hamas on the ground. In this regard, as the ceasefire negotiations neared their endgame, Israel's Defense Minister Ehud Barak rightly noted: "Hamas will not disappear, but the memory of this experience will remain with it for a very long time, and this is what will restore deterrence."[49]

This latest flare-up of hostilities between Israel and Hamas and the successful IDF response highlighted two additional windfall benefits that ultimately accrued to Israel from Operation Change of Direction in 2006. First, Hizbollah watched the unfolding of Israel's eight-day pummeling of Hamas throughout the November fighting with keen interest as the Iron Dome system largely spared the country's civilians from substantial harm by Hamas rocket fire until the ceasefire was implemented.[50] However, it studiously avoided any attempt to open a second front on Israel's northern border by joining Hamas in contributing to the rocket fire. That restraint suggested that Israel's deterrent against Hizbollah not only remained intact but may have been even further enhanced by Iron Dome's impressive performance.

True enough, shortly after the fighting between Israel and Hamas ended, Nasrallah warned ostentatiously that his combatants would unleash "thousands" of their own rockets against Tel Aviv and Jerusalem in the event of any future war between Israel and Hizbollah. Yet in a resounding affirmation that actions speak louder than words, Hizbollah took care not to undertake any actual physical provocation against Israel that might risk inviting another massive retaliation by the IDF against its assets throughout Lebanon. Moreover, as before in the years since the Second Lebanon War, Nasrallah issued his bombastic but otherwise hollow threat not in public, but through the safety of a video link from an undisclosed location.[51]

Second, in a notable departure from six decades of previous Israeli military practice, the revealed shortcomings in the IDF's performance in Lebanon in 2006 gave rise, perhaps for the first time, to a serious "lessons-learned" undertaking on the part of Israel's military leaders. That determined effort had a clear positive impact on the course and outcome of the IDF's first Gaza war two years later. It may also have revealed its full consummation in the IDF's second round of successful combat against Hamas in November 2012. Two years before, an informed and thoughtful Israeli scholar suggested that Israel's military culture had yet to assimilate

"formalized systems for learning lessons from its campaigns" and that any successes the IDF may have achieved at drawing useful conclusions from its past combat experiences tended to be mainly of a narrow technical and tactical nature.[52]

Yet in the early aftermath of its flawed Lebanon campaign in 2006, the IDF under General Haloutz's personal direction carried out a determined and brutally honest effort involving all three branches over a course of six months to understand and assess what went wrong in the conduct of Operation Change of Direction. In short order, that effort led to significant improvements in air-ground integration and joint campaign planning that in turn eventually resulted in the substantially more effective Israeli performance in Operations Cast Lead and Pillar of Defense.[53] Each of the above-noted developments was a direct linear outgrowth of the IDF's performance against Hizbollah in 2006, further underscoring the extent to which, viewed with the benefit of six years' hindsight, Israel's security situation gained in the long run from the experience of the Second Lebanon War.

In a summary statement to the Winograd Commission that well captured the case for this more encouraging outlook across the board, General Haloutz declared as early as January 2007: "When I judge the results [of the campaign] in light of the goals [of the campaign], and when I look at the military outcome where an improved military situation has been created, where Hizbollah has been weakened, and where the Lebanese establishment has understood that it must implement its responsibility over Lebanon...I think that...the starting point today is substantially superior to what it was before the outbreak of the fighting. I cannot tell how long this will last, but what I can say is that even today, this is the longest period of time ever in which such a reality has existed along the border.... From the military point of view, [Hizbollah] has been dealt a blow like it had never felt before."[54] Thus far, that early optimistic appraisal has been amply borne out by Hizbollah's subsequent cautious behavior throughout the ensuing years.

Notes

1 Amos Harel and Avi Issacharoff, *34 Days: Israel, Hezbollah, and the War in Lebanon* (New York: Palgrave Macmillan, 2008), p. ix.

2 For more on this point, see Benjamin S. Lambeth, "An Airpower Failure? Hardly!," *Aviation Week and Space Technology*, October 10, 2011, p. 70.

3 On the second of these two counts, in testimony before the Knesset after the initial week of fighting, the IDF chief reported that Hizbollah was seeking to draw Israel into a prolonged war of attrition and that while the IDF had plans in hand for a ground counteroffensive, it was not yet ready to implement them because of the near-certainty of high friendly troop casualties that any such move would generate. See Abraham Rabinovich, "Hezbollah Trained for Six Years, Dug Deep Bunkers," *Washington Times*, July 21, 2006.

4 These two extravagant goals, both unattainable by any military means that Israel's rank and file would likely have countenanced, were announced by Olmert six days into the campaign in a speech to the Knesset that showed no sign of any serious prior strategy deliberation. See Harel and Issacharoff, *34 Days*, pp. 107-8. Notably, they were *not* among the more modest campaign goals that the IDF General Headquarters had formally assigned to Israel's fighting forces at the start of Operation Change of Direction.

5 A fuller development of this argument is presented in Benjamin S. Lambeth, *Air Operations in Israel's War against Hezbollah: Learning from Lebanon and Getting It Right in Gaza* (Santa Monica, CA: RAND Corporation, 2011), http://www.rand.org/pubs/monographs/MG835.html.

6 William M. Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War* (Maxwell AFB, Ala.: Air University Press, 2007), p. 147.

7 "Testimony by Lieutenant General Dan Haloutz, IDF Chief of Staff, to the Winograd Commission Investigating the Second Lebanon War," unpublished English translation from the Hebrew, Jerusalem, Israel, January 28, 2007. The commission was named for its appointed chairman, Judge Eliyahu Winograd, a retired president of the Tel Aviv District Court.

8 Ibid. Israel's first Lebanon War, which began in 1982 and ended fully with Israel's withdrawal in 2000, resulted in nearly 600 IDF troops killed over the course of its 18-year duration. It has since been widely regarded as Israel's Vietnam.

9 Interview with Brigadier General Itai Brun, IAF, Director, Dado Center for Interdisciplinary Military Studies, Camp Glilot, Herziliya, Israel, March 26, 2008.

10 Dan Haloutz, *At Eye Level* (Tel Aviv: Yediot Books, 2010), from an unpublished English translation.

11 For a fuller development of this line of argument, see Eyal Zisser, "Nasrallah's Defeat in the 2006 War: Assessing Hezbollah's Influence," *Middle East Quarterly* 16, no. 1 (2009): 27-35.

12 For more on these two operations, see Lambeth, *Air Operations in Israel's War against Hezbollah*, pp. 29-36. In a rare public speech from an undisclosed location through a video link on July 18, 2012 in celebration of the sixth anniversary of his proclaimed "divine victory" over Israel, Nasrallah made a special point to address the IAF's preemptive attack against Hizbollah's hidden medium range rockets and denied that the air offensive was mission-effective. He claimed that his organization "knew that Israel knew where the

platforms were located" and accordingly managed in due time to "change the location of these platforms without allowing the Israelis to find out" – as if saying so made it so. Quoted at "Sayyed Hassan Nasrallah," *Now Lebanon*, http://www.nowlebanon.com/NewsArchiveDetails.aspx?ID=420450.

13 Amir Kulick, "The Next War with Hizbollah," *Strategic Assessment* 10, no. 3 (2007): 41-50.

14 Isaac Ben-Israel, *The First Israel-Hizbollah Missile War* (Tel Aviv: Program for Security Studies, College of Policy and Government, Tel Aviv University, May 2007), p. 19 of an unpublished translation into English.

15 Martin Van Creveld, "Israel's Lebanese War: A Preliminary Assessment," *Journal of the Royal United Services Institution*, October 2006, p. 43.

16 For amplification, see Ronen Manelis, "Between Lebanon and Gaza: Hizbollah in Operation Cast Lead," *Military and Strategic Affairs* 1, no. 1 (2009): 43-50.

17 Ben Caspit and Jackie Hugi, "Speech of the Panicked Mice," *Maariv*, September 25, 2006.

18 Ibid.

19 Colum Lynch and Robin Wright, "Peace Resolution for Lebanon Unanimously Approved at UN," *Washington Post*, August 12, 2006.

20 Steven Erlanger, "Israel Committed to Block Arms and Kill Nasrallah," *New York Times*, August 20, 2006.

21 Gabriel Siboni, "From Gaza to Lebanon and Back," *Strategic Assessment* 10, no. 1 (2007): 66-69.

22 Cited in Guermantes E. Lailari, "The Information Operations War between Israel and Hizballah during the Summer of 2006," in James J. F. Forest, ed., *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas* (Westport, Conn.: Praeger Security International, 2009), p. 322.

23 Greg Myre and Helene Cooper, "Israel to Occupy Area of Lebanon as Security Zone," *New York Times*, July 26, 2006.

24 "Hezbollah Chief Revisits Raid," *Washington Post*, August 28, 2006.

25 Thomas L. Friedman, "Not So Smart," *New York Times*, July 19, 2006.

26 Ben-Israel, *The First Israel-Hezbollah Missile War*.

27 Cited in Jim Storr, "Reflections on the War in Lebanon," *Journal of the Royal United Services Institution*, April 2007, p. 71.

28 For more on this point, see Benjamin S. Lambeth, "Forging Jointness under Fire: Air-Ground Integration in Israel's 2006 War against Hezbollah," *Joint Force Quarterly* 66, no. 3 (2012): 48-53.

29 Ron Tira, "Shifting Tectonic Plates: Basic Assumptions on the Peace Process Revisited," *Strategic Assessment* 12, no. 1 (2009): 91-107, especially pp. 100, 102.

30 Sanu Kainikara and Russell Parkin, *Pathways to Victory: Observations from the 2006 Israel-Hezbollah Conflict* (Canberra: Royal Australian Air Force, Air Power Development Centre, October 2007), p. 17.

31 Andrew F. Krepinevich, Jr., "The Pentagon's Wasting Assets: The Eroding Foundations of American Power," *Foreign Affairs*, July/August 2009, p. 24.
32 Tira, "Shifting Tectonic Plates," p. 102.
33 Roni Bart, "The Second Lebanon War: The Plus Column," *Strategic Assessment* 9, no. 3 (2006): 16-17.
34 Ben Caspit, "First, Let's Win," *Maariv*, August 11, 2006.
35 For more on this, see Gabriel Siboni, "From the Second Intifada through the Second Lebanon War to Operation Cast Lead: Puzzle Pieces of a Single Campaign," *Military and Strategic Affairs* 1, no. 1 (2009): 25-33, especially pp. 28-29.
36 Itai Brun, "The Second Lebanon War as a 'Wake-Up Call': A Strategic Perspective and Major Lessons Learned," Camp Glilot, Herziliya, Israel: Dado Center for Interdisciplinary Military Studies, undated briefing charts.
37 Michael Oren, "Time Is Short for Iran Diplomacy," *Wall Street Journal*, August 7, 2012.
38 Bret Stephens, "Plotting the Next Mideast War," *Wall Street Journal*, April 10, 2010.
39 Ronen Bergman, "Israel's Secret War on Hezbollah," *Wall Street Journal*, October 10, 2009.
40 Al-Manar television (Beirut), February 13, 2009.
41 Some have suggested that the attack by a confirmed Hizbollah suicide bomber that killed five Israeli tourists in Burgas, Bulgaria on July 18, 2012 may have been intended as retribution for Mughiyeh's assassination. A more plausible explanation for that particular incident, however, is that the attack was a directed retaliation for the assassinations of Iranian nuclear scientists, for which Iran, Hizbollah's main sponsor and manipulator, has blamed Israeli agents. See Nicholas Kulish and Eric Schmitt, "Hezbollah is Blamed for Attack on Israeli Tourists in Bulgaria," *New York Times*, July 19, 2012.
42 Bergman, "Israel's Secret War on Hezbollah."
43 Ibid.
44 Ibid.
45 Howard Schneider, "Israel Finds Strength in its Missile Defenses," *Washington Post*, September 19, 2009.
46 Yaakov Katz, "Iron Dome Successfully Intercepts Kassam, Katyusha Barrages," *Jerusalem Post*, July 15, 2010.
47 Sheera Frenkel, "Israel Sees New Advantage in Iron Dome Anti-Missile System," *McClatchey*, March 26, 2012.
48 On this count, after the relative quiescence for a time that followed the successful conclusion of Operation Cast Lead in January 2009, there were 365 rocket and mortar attacks from Gaza into southern Israel in 2010, 680 in 2011, and 800 through most of 2012, with 171 in October alone. (Peter Beinart, "Israel's Fatal Game," *Newsweek*, November 26, 2012.) Of the IAF's eventual response to these provocations, IDF Colonel (ret.) Gabi Siboni said:

"Deterrence has to be maintained. It was only a question of time until this moment arrived." See Isabel Kershner and Fares Akram, "Ferocious Israeli Assault Kills a Leader of Hamas," *New York Times*, November 15, 2012.

49 Nidal al-Mughrabi and Jeffrey Heller, "Israel, Gaza Ceasefire Agreed to, Hamas Official Says, Israel Denies," *Reuters*, November 20, 2012.

50 Throughout the operation's eight days, Hamas fired a total of 1,506 rockets into Israel from the Gaza Strip. Of those that were determined to have been headed toward populated areas, Iron Dome intercepted and stopped 421, with only 58 landing in urban settings, making for an overall success rate of nearly 90 percent and only 5 Israeli fatalities occasioned by the rocket fire. See "IDF Newsletter: IDF Ends Operation Pillar of Defense," from newsletter@idfblog.com, November 21, 2012.

51 Bassem Mroue, "Hezbollah Chief Says Rockets Would Hit Tel Aviv in War," *Washington Post*, November 26, 2012.

52 Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors in the Revolution in Military Affairs in Russia, the U.S., and Israel* (Stanford, CA: Stanford University Press, 2010), p. 124.

53 For an assessment of how this focused effort paid off in the IDF's planning and conduct of Operation Cast Lead, see Benjamin S. Lambeth, "Israel's War in Gaza: A Paradigm of Effective Military Learning and Adaptation," *International Security* 37, no. 2 (2012): 81-118.

54 "Testimony by Lieutenant General Dan Haloutz, IDF Chief of Staff, to the Winograd Commission Investigating the Second Lebanon War."

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).

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/.

Iran and Cyberspace Warfare

Gabi Siboni and Sami Kronenfeld

Introduction

Throughout the world decision makers and the general public have undoubtedly realized in recent years that cyberspace must be treated as a genuine realm of warfare. As such, it allows considerable room for maneuvering and has vulnerabilities that can be breached by hostile elements seeking to derail information systems or even inflict physical damage on critical infrastructures controlled by industrial control systems. In the wake of this new understanding, many countries are investing increasingly in safeguarding their cyber resources (particularly in the fields of defense, intelligence gathering, and offense capabilities). Since the Stuxnet attack – one of the most destructive cyber attacks to date – Iran has been working hard to improve its cyberspace defenses on the one hand, while building up cyberspace intelligence gathering and offensive capabilities on the other.

The Iranian cyberspace defense program has a dual objective: first, it hopes to prevent another attack like Stuxnet and intelligence-directed penetration of Iranian computers by viruses such as Duqu and Flame. In this sense, the goal of the Iranian program is similar to that of many other nations seeking to protect their critical infrastructures. The second objective is the regime's desire to ensure its survival by means of surveillance and blocking of information and services originating with the Iranian public. In many cases the two goals are achieved with the same tools, e.g., the Iranian effort to create a separate Iranian web or the disabling of Google services in that country.[1]

Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and the Cyber Warfare program at INSS. Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS.

At the same time, Iran is also in the midst of a concerted effort to construct offensive capabilities, on the assumption that in any future confrontation the use of cyberspace will have a critical impact on achieving success against the enemy. Gathering information openly about Iranian cyberspace capabilities, especially offensive ones, is by definition extremely difficult. But the country's cyberspace activities have recently been in the spotlight because of suspicions of Iranian involvement in some serious cyberspace incidents, including the theft of internet security permissions, an attack on the Saudi Arabian oil company's organizational network, and not least, the penetration of computers at some leading American banks.

This article examines the current situation regarding various elements of Iran's cyberspace development process. The first section analyzes the country's cyberspace strategy, while the second section describes the organizational and operational response to the formulated strategy. This comprises three components: infrastructures for training and developing technological manpower for work in cyberspace; technological developments that have already been introduced; and the overall processes of cyberspace force construction. Finally, the article focuses on a number of cyberspace incidents attributed to Iran, attempts to gain some insight into the way Iran conducts its cyberspace activities, and examines implications for Israel and other Western nations.

Iran's Cyberspace Strategy

The role of the communications and information networks in the outbreaks that followed the 2009 Iranian presidential election and those that erupted as part of the "Arab Spring," as well as the cyber attacks on Iran made the cyberspace arena tremendously important to the Iranian regime's overall security doctrine. Evidence of the subject's significance in the minds of Iran's decision makers was proffered by none other than the Supreme Leader himself, Khamenei, in a direct reference to the opportunities and dangers of cyberspace when, in March 2012, he announced the establishment of a Supreme Cyberspace Council composed of senior government representatives charged with planning and implementing a single integrated cyberspace strategy.[2] While the work of this Council began only quite recently, an analysis of Iranian cyberspace activity in recent years indicates the existence of an Iranian cyberspace strategy with clear goals and objectives.

Two fundamental assumptions underlie Iran's approach to its modus operandi in cyberspace. The first concerns the development of defensive capabilities to withstand attacks by hostile nations and entities, alongside the development of operational capabilities against opponents of the regime on the home front; the second concerns the development of offensive capabilities to enable Iran to combat what it sees as American superiority and control of global internet capabilities and infrastructures.

In the defense arena, Iran is working to accomplish two main goals in cyberspace.[3] First, it aims at an effective, comprehensive, advanced technological protective system to defend critical infrastructures and sensitive data against cyber attacks such as Stuxnet, which compromised the Iranian uranium enrichment program and shut down more than 1,000 centrifuges at the enrichment facility in Natanz.[4] Second, Iran is trying to curb and foil the cyberspace activities of domestic opposition parties and opponents of the regime, for whom cyberspace is an important communications platform for disseminating information and organizing anti-government activities. In addition, the regime hopes to prevent the cyberspace penetration of Western ideas and information that conflict with its interests, thereby blocking "soft revolution" processes that are liable to damage the regime's stability and hold on the state. In the context of defensive capabilities, the news about Iranian plans to develop a separate, independent communications network is noteworthy.[5] Although this has at times been denied by Iranian officials,[6] as time goes by it seems to take on more validity.[7]

On the offensive front, Iran's cyberspace strategy sees this arena first and foremost as central in the asymmetrical doctrine of warfare, a key principle in Iran's perception of the use of force. Iran sees cyberspace warfare, in a similar way to more obvious asymmetrical tactics such as terrorism and guerilla warfare, as an effective tool to inflict significant damage on the enemy's home front with military or geostrategic superiority. Experts estimate that in the event of an escalation in the confrontation between Iran and the West over the Iranian military nuclear program, Iran would attempt a cyber attack against major infrastructures – such as power plants, financial institutions, and transportation systems – on American soil.[8] An article published in July 2011 in the Iranian newspaper *Kayhan* (which is closely identified with Khamenei) hinted at such a possibility by warning

that the United States must take care lest "an unknown player somewhere in the world" carry out an attack on its most vital infrastructures.[9]

Beyond the military-strategic aspect, the Iranian regime and its supporters also use offensive cyberspace warfare to impair the cyber activities of Western countries and opponents to the regime in Iran. Iranian hackers, who usually have no official affiliation with the establishment but are linked to it nonetheless, consistently engage in cyber attacks causing internet crashes, inserting pro-Iranian material, stealing information, committing credit card fraud, damaging service providers, and rerouting internet traffic.[10] Propaganda is another part of the cyberspace warfare strategy. The Iranian regime understands well the importance of cyberspace in shaping the points of view and attitudes of large groups of people inside Iran and abroad, and invests major efforts in creating a sizable and effective propaganda machine extolling the regime and maligning its enemies. To realize these strategic goals, Iran is investing considerable resources in creating a tight, skilled, multi-layered structure that includes impeding, monitoring, controlling, and offensive capabilities in cyberspace.

Iran's Organizational and Operative Response

With its cyberspace strategy goals in mind, Iran set about applying itself vigorously to strengthening its cyberspace capabilities. There are reports of investments amounting to some $1 billion in the development and acquisition of technologies and in recruitment and training of experts to advance and strengthen both defensive and offensive cyberspace capabilities.[11] There are various interconnected components in the processes of building an operative and organizational cyberspace response: first, building up a training and development manpower base at research institutes and institutions of higher education; second, efforts towards large scale technological development; and third, processes of force buildup, including development of a doctrine, establishment of organizations, and formulation of a hierarchy of authority to implement the doctrine.

Manpower Training and Development

The infrastructures for the technological training and development of Iranian cyberspace are found primarily in the country's universities and technological institutes. Iran has many institutions of higher education and academic research engaged in research and training in the fields of

IT, computer engineering, and communications.[12] Leading universities in this area include: Sharif University of Technology in Tehran, offering advanced degrees in computer engineering, electronic engineering, and mathematics,[13] and which is also the site of two advanced research institutes in communications and information technologies (the Advanced Information and Communication Technology Center[14] and the Advanced Communication Research Institute[15]); and Amikabir University of Technology, also in Tehran, with large departments of mathematics, computer sciences, computer engineering, and information technology. It seems that Amikabir specializes in data security; the computer engineering department offers several advanced courses in security information,[16] and also operates a research lab specializing in data security[17] and a separate research lab specializing in secure systems analysis.[18]

In addition to academic research and training, the Iranian regime invests significant sums in the promotion and support of IT and computer communications companies. Such investments are made directly by government organizations such as the Science Ministry, and indirectly via the financing and establishment of greenhouses for hi-tech companies in which the government has an interest.[19] The Iran Telecommunications Research Center is a key government body in the IT field; it specializes in research in information and communications technology and is the research and professional arm of the Information and Communications Ministry. The center operates and trains advanced research teams in many fields, including data security.[20] Another government body promoting research in IT is the Technology Cooperation Office, which belongs to the Presidential Bureau. Its stated objective is to improve technological cooperation with other nations. It directs and initiates research projects in many areas, including information technologies.[21] The EU and other Western sources have singled it out as being involved in the nuclear program.[22]

Apart from direct investments by government bodies, the Iranian regime also operates hi-tech greenhouses engaged in data security research. Prominent among such hi-tech centers is the Pardis Technology Park, also known as the Iranian Silicon Valley. Established in 2001 by the Presidential Bureau and the Technology Cooperation Office, it houses more than 400 companies involved in communications and IT.[23] Another hi-tech greenhouse is Guilan Science and Technology Park, a support center for

startups and home to a number of companies working on information security.[24]

Technological Empowerment

Beyond developing and training a strong cyberspace workforce, Iran has also been focusing on technology to promote its strategic goals in cyberspace. One target of major investment is intra-state cyberspace and information flow. In recent years, the Iranian regime has bought and developed advanced technological systems allowing it to conduct surveillance and monitor information traffic on computer and mobile networks in the country. The largest government controlled telecom corporation (the Telecommunications Company of Iran) bought a surveillance system from the Chinese ZTE Corp. The system, capable of monitoring information on telephone lines, computer networks, and cellular lines, was acquired as part of a comprehensive deal between the two companies estimated at $130 million. The deal covered products of the ZMXT system, which the Chinese company describes as an integrated monitoring system. The products purchased enable voice communications eavesdropping, text message surveillance, and monitoring of web surfing.[25]

In addition to surveillance and monitoring, the Iranian government is also developing website blocking and filtering technologies, since international sanctions prevent Iran from buying Western-manufactured data filters. Amnafzar Ltd., an IT company with links to the regime, developed a data filter called Separ, which is updated constantly and frequently changes its filtering strategy so as to evade efforts to circumvent it.[26] Using this technology, the regime has succeeded in significantly limiting the flow of information into and within the country. Research published in March 2009 by the OpenNet Initiative (a joint project by a number of institutions, including Harvard University and the University of Toronto) identified Iran as one of the leading nations in website filtering and blocking, alongside nations such as China, North Korea, Syria, and Myanmar.[27]

These technologies allow Iran relatively close control of the state's cyberspace, but the regime nonetheless strives for outright control of information, ideas, and access to Iranian cyberspace. To this end Iran embarked on a project of establishing an independent and separate national network, isolated from the World Wide Web. The idea is that the

establishment of this national web, named Halal, will allow the regime full control of contents for public exposure and will also cause serious damage to opponents of the regime conducting widespread activities on the internet. It will also make virus attacks and other cyber attacks on Iranian infrastructures much more difficult. The national network project first came into being in 2009, when the Iranian authorities instructed domestic companies to move their network activities to servers and data centers on Iranian soil. During 2012 it was reported that Iran is developing an internal email service, an independent operating system, a search engine, and other tools for use on the new network.[28] In August 2012 Iranian Communications Minister Reza Taghipour announced that Iran would disconnect from the World Wide Web within 18 months.[29] However, Western experts believe it will be difficult for the regime to sever all connections with the global network.[30]

Iran is also seeking to isolate networks in the security establishment and construct a national intelligence communications network separate from the global web.[31] The first indication of this effort is Basir, the intra-organizational network of the Revolutionary Guards, whose existence became public knowledge in March 2012. Reports describe it as a closed cellular network, possibly operated by designated relay stations. The network supposedly affords the organization efficient, encrypted lines of communication, even in a scenario of a comprehensive cyber attack on the country's communications and information infrastructures. Thus far it is unclear if it is also an information network or a voice system only.[32]

Force Buildup

As for cyberspace force buildup processes, the many training and development facilities available to Iran have allowed the Islamic Republic to establish a large cyberspace configuration with multiple capabilities, both defensive and offensive. In the last decade, Iran embarked on a strategic expansion of its national cyber constellation, with cyberspace agencies and organizations established for almost every relevant government ministry. The goal is to create a hierarchical and diverse organizational alignment with a clear plan of action, well thought out resource allocations, distribution of responsibility and the ability to preserve and disseminate information, know-how, and data.

The crowning glory in the construction of Iran's cyberspace force is the establishment of the Supreme Cyberspace Council. The Council was set up in March 2012 at the behest of Supreme Leader Ayatollah Khamenei and serves as the ultimate authority on all of the nation's cyberspace issues.[33] The Iranian President heads the Council and its members comprise senior government representatives and others, including the senior commander of the Revolutionary Guards, the head of the Majlis, the Ministers of Science, Communications and Culture, the chief of police, and the president of the Islamic propaganda organization. The Council has the authority to determine national cyber policy and its directives are binding on all Iranian institutions operating in the field. The Council plans to establish a National Cyber Center under its auspices, to integrate all Iranian cyberspace activity, gather and disseminate information and instructions, and oversee the enforcement of the Council's directives by all relevant bodies.

Iran's cyberspace structure comprises many cyberspace organizations working in various fields and officially affiliated with establishment organizations. One central organization with a defensive orientation is the Cyberspace Defense Command, which operates in the context of the Passive Defense Organization belonging to the general staff of the armed forces.[34] Alongside military personnel, this cyberspace organization also comprises government ministry representatives (the Communications, Defense, Intelligence, and Industry ministries). Its main objective is to develop a comprehensive defensive doctrine for state institutions and infrastructures against cyber threats.[35] The organization is primarily defensive, and currently does not seem to be involved in offensive cyber activity.

Another defensive cyberspace entity is the Center for Information Security, known as MAHER, established and operated as part of the Communications and Information Technologies Ministry. This center is primarily responsible for activating computer security incident response teams in the event of emergencies and cyber attacks. In addition, the center trains skilled manpower, develops response mechanisms to cyber crises, and stores and disseminates data security know-how. It is responsible for defending all government websites, as well as those of private companies operating officially and listed with the Communications Ministry. The center's teams were called on to impede and foil the work of the Flame and Stuxnet viruses that attacked Iran.[36]

Other cyberspace organizations focus on enforcement and control of intra-Iranian cyber activities that run counter to the regime's interests. In July 2009, the Supreme Council of the Cultural Revolution, which is subject to the supreme leader, founded the Committee to Identify Unauthorized Websites. Among its members are the Attorney General, the chief of police, the supervisor of government media, and various government ministers (from the Intelligence, Communications, Culture, and Science ministries, among others). The committee's purpose is to identify websites whose contents and activities are incompatible with the regime's requirements and wishes, and it is authorized to block access to such sites.[37] In 2011, the police established its own cyberspace unit, FETA,[38] to combat cybercrime – fraud, data theft, threats, and so on – but it is also authorized to take action against political and security criminals in cyberspace, and it is actually this latter task that primarily occupies it.[39] In addition, FETA is further charged with monitoring and controlling internet users in Iran, especially those in internet cafes around the country, where web surfing can be relatively anonymous.[40]

As for the offensive capabilities of Iran's cyberspace resources, the picture is less clear. Naturally, the Revolutionary Guards are crucial in the establishment and operation of offensive cyberspace warfare. Western experts place Revolutionary Guards capabilities in the top tier of cyberspace warfare worldwide.[41] A 2008 analysis by the research institute Defense Tech[42] estimated that the Revolutionary Guards cyberspace warfare program employed some 2,400 professionals and at that time had a budget of $76 million. Among capabilities that Defense Tech attributed to the Revolutionary Guards were: developing infected software by inserting malicious codes into counterfeit computer software; developing capabilities to block communications and WiFi networks; developing malicious codes (viruses and worms) capable of reproducing in networks and attacking target computers; developing tools for penetrating computers and networks to gather intelligence and pass it on to remote servers; and developing delay mechanisms installed in target computers to be operated by a predetermined schedule or by command from control servers.

In addition to information warfare capabilities, the Revolutionary Guards are also creating an electronic warfare system capable of blocking radar and communications. The organization is investing large sums in

the acquisition of electronic warfare systems[43] that, in conjunction with existing cyberspace warfare capabilities, will serve as an effective tool for compromising the electronic systems of the United States and its allies during a military confrontation.[44] According to declarations by the Revolutionary Guards, Iran has exhibited its prowess in the realm of cyberspace warfare with the capture of an unmanned aerial espionage vehicle in December 2011.[45]

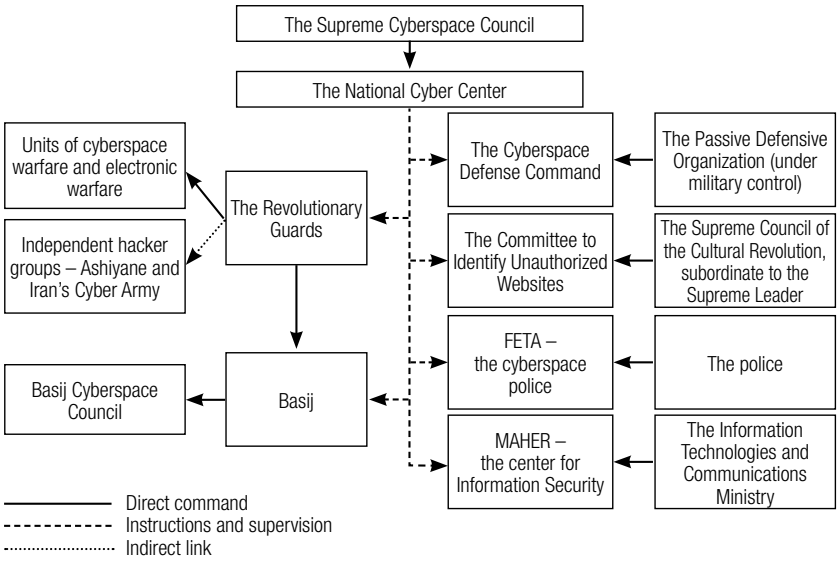
Other than the Revolutionary Guards cyberspace warfare units, there is evidence linking the Revolutionary Guards and groups of Iranian hackers active against domestic and global enemies of the regime. The use of outsourcing allows the Revolutionary Guards and Iran to maintain distance and refute any allegations of Iranian involvement in cyberspace warfare and cybercrime. Experts have identified one group of Iranian hackers involved with the Revolutionary Guards as the Ashiyane Digital Security Team,[46] whose members are motivated by an ideology supporting the Iranian regime and the revolution, and who aim their attacks at the regime's enemies. The Ashiyane Team trains hackers and gives them significant capabilities,[47] which are then used for political activities (including the insertion of pro-Iranian propaganda into Western and Israeli websites and causing them to crash), as well as criminal enterprises (credit fraud, identity theft, and infiltration of databases and financial institutions). Furthermore, the group hosts a forum called War Games, which holds hacker competitions whose targets include American infrastructures companies.[48]

Another hacker group believed to be linked to the Revolutionary Guards is Iran's Cyber Army,[49] which consists of hackers and computer experts using fictitious identities and declaring themselves part of an organization. The group's main activities include breaking into Western websites with the aim of inserting pro-Iranian contents, seizing control of and redirecting information traffic, infiltrating Western data security companies, and damaging websites of the regime's opponents.

The Basij organization, which is subordinate to the Revolutionary Guards, has also become active in cyberspace and in 2010 established the Basij Cyberspace Council. Basij focuses primarily on creating pro-Iranian propaganda in cyberspace. It recruits and trains thousands of Iranians to write contents, afterwards deploying organized computer groups for tens of thousands of pro-regime bloggers. They also write talkbacks and other

materials supporting the regime in the new media, on major forums, and on websites in Iran and abroad.[50] Nevertheless, Basij plans to further advance its cyberspace capabilities and is using experts from the Revolutionary Guards' cyberspace units to train hackers with high offensive capabilities.[51]

All of this clearly illustrates that in recent years Iran has established an extensive cyberspace structure encompassing many areas of activity, and has a wide range of capabilities at its disposal. The organizational flowchart below demonstrates the hierarchical configuration of the state's cyber establishment, as described above.



Clearly there have been significant advances in Iran's cyber activities. On the defense front all energies are focused on creating a defensive and isolation capability adequate for coping with any attempts at infiltrating the country's vital networks and infrastructures. Although it is hard to gain an entirely reliable picture of the development of offensive cyber capabilities, the following section of this article looks at several such activities.

Cyberspace Activities Attributed to Iran

In December 2011, an expose broadcast in an investigative program on the Univision television network led to an American inquiry into the involvement of official Iranian personnel in a cyber plot against the United States. The network's investigative reporters managed to infiltrate a group

of Mexican hackers operating against US targets and secretly videotaped a meeting between their representatives and the Iranian Ambassador to Mexico. At the meeting, held at the Iranian Embassy, the hackers asked about the possibility of receiving support and financing from the Iranian government in order to carry out cyberspace attacks on American targets, such as the Pentagon, the CIA, the FBI, and various American nuclear installations. The video shows then-Iranian Ambassador to Mexico Muhammad Hassan Ghadari asking questions and proposing additional courses of action. The Ambassador stressed that Iran wants information on the possibility of an American attack on Iran. At the end of the conversation, he expressed his desire to stay in touch with the hackers and promised to forward the proposal to his superiors.[52] It may be assumed that this attempt was not an isolated one and that Iran is actively recruiting hackers and others around the world to further its offensive cyberspace goals.

A decisive determination of the identity of cyberspace attackers is complex and requires resources and international cooperation. Therefore, it is hard to say with absolute certainty who is behind many cyberspace actions. Nonetheless, it is often possible, using circumstantial diagnostics, to identify those responsible with a high degree of certainty. This article highlights three incidents: an attack on two data security companies aimed at stealing security permissions; an attack on large financial institutions in the United States; and an attack on the Saudi Arabian oil company Aramco.

The Attack on DigiNotar and Comodo

In 2011 two attacks took place on companies providing SSL (secure sockets layer)[53] permissions. The first, in March 2011, targeted the American company Comodo Ltd. Several permissions were stolen, among them domain permissions of internet mail services such as Google, but these were withdrawn before being used by the attacker. In fact, someone with authority in the mail.google.com domain can steal Gmail passwords and hijack users' accounts. Someone with a stolen authorization for the Microsoft.com domain can install malicious software in victims' computers. According to the company, the following findings came to light about this incident:[54]

a. The attack lacked features typical of cybercrime.
b. The attackers were organized and knew precisely what they were seeking before the attack, indicating the involvement of a state organization in the attack.

c. The source of the attack was primarily Iran (based on identification of the IP address).
d. The website where the stolen permissions were checked is located in Iran and was immediately removed from the web after Comodo discovered the attack.

The attack on Comodo failed to achieve its goal: it was identified and neutralized before the stolen permissions could be used. However, this was not the case with DigiNotar, the major Dutch SSL permissions provider. The company's databases came under attack from June through August 2011. During the attack, which came to be known by the name Black Tulip, certifications for website verification were stolen, including the certification serving to verify the google.com domain, thus allowing the attacker to assume this identity and reroute Gmail servers.[55]

An analysis ordered by DigiNotar (which went bankrupt and shut down operations after the attack) showed that 531 certificates were stolen and fabricated and that most stolen permissions were used to penetrate users' email accounts, especially in Iran. The analysis further revealed that the attack managed to penetrate more than 300,000 computers, which were overwhelmingly Iranian (more than 99 percent).[56] It is hard to determine the source of the attack with absolute certainty, but experts believe that it was Iran and that it was apparently intended for internal security purposes.[57] What led to this conclusion were the targets and extensive scope of users attacked and messages left on the company's website indicating Iranian involvement in the attack.

The Attack on American Financial Institutions

A report issued in the United States in September 2012 shows that at around the same time, several US financial institutions also came under attack, including sites belonging to the Bank of America, Morgan Chase, and Citigroup. Assessments by American sources concluded that the cyber attacks against the American financial institutions did not originate from random hackers, but were most likely financed by Iran and carried out by way of retaliation against sanctions imposed on Iran by the United States.[58]

As a result, the Financial Services Information Sharing and Analysis Center[59] issued an alert to banks in the United States about cyber attacks designed to steal identities via email, Trojan horses, and malicious tools for registering keystrokes and to retrieve user and employee names and

passwords. Although large banks were also attacked, most of the victims were small and medium businesses, small banks, and credit companies. A group called the Izz ad-Din al-Qassam Cyberspace Fighters announced that it had attacked the Bank of America and the New York Stock Exchange in retaliation for a September 2012 movie expressing disrespect for the prophet Muhammad. These attacks, as described in the warning, indicate that the attackers succeeded in obtaining a great deal of information from the banks' networks, at least in some cases, and also accessed employees' entry permissions, thereby circumventing defensive mechanisms.[60]

The Attack against Aramco

In August 2012, apparently with insider help from someone with a high level of access to company computers, some 30,000 computers belonging to the Saudi Arabian oil company Aramco and the Qatari natural gas company ResGas were attacked by a computer virus called Shamoon. According to experts, this was one of the most devastating attacks carried out against any single company. The virus spread through the company's servers and attacked information stored in them. In-house computer experts say that the damage was limited to office computers and did not affect the company's operational and control systems.[61]

Symantec identified the virus for the first time in August 2012. An analysis by their experts and other security companies reveals the following findings:[62]

a. The Shamoon virus was designed to attack computers of an organizational computerized system (IT) rather than a control system. The virus is not in the same category of sophisticated cyberspace warfare tools such as Stuxnet, which attacked the Iranian nuclear program in 2010.
b. The purpose of the viral attack was not espionage or intelligence gathering but rather the complete and total destruction of data and target computers.
c. The writers of the malicious code do not seem to belong to the top tiers (such as the writers of Stuxnet and Flame), and there are indications that those behind it do not have a very high professional profile, since it was riddled with coding errors. They were, on the other hand, skilled enough to create a particularly destructive code.

d. The virus penetrated the company's computers with the help of a collaborator inside the company with direct access to the system and who seems to have used a USB device for the purpose.
e. The writers of the code used a section of a picture of a burning American flag to hide the contents of the files in the infected computers, indicating a political and/or religious (Islamic) affiliation.
f. The code of Shamoon's deletion mechanism contained the word Wiper. A similar name was used in the virus code of Flame, which attacked the Iranian oil company. This parallel raises a suspicion that the attack on Aramco was an Iranian retaliation to the Flame attack.

A group called The Cutting Sword of Justice claimed responsibility for the Aramco attack, declaring it was aimed at the main source of income in Saudi Arabia, a country accused of committing crimes against Syria and Bahrain. The group further claimed that the virus allowed it to access many secrets, but to date no relevant information on the issue has been reported. Reports on similar attacks on oil and gas companies in the Persian Gulf raised suspicions that the attacks were part of a concerted national effort. US Secretary of Defense Leon Panetta recently hinted at Iranian involvement in the attack. A former senior member of the American administration spoke out more directly when he claimed the administration believes Iran was behind the attacks in the Gulf.[63]

An analysis carried out by American cyberspace security expert Jeffrey Carr[64] raises a number of allegations linking Iran to the attack. It is the only country with access to the original Wiper code, which seems to have formed the basis for the Shamoon virus. According to a report issued by Kaspersky,[65] the Wiper code used in the attack on the Iranian Energy Ministry in April 2012 was also used by Shamoon's creators. Iran is highly motivated to attack the Saudi Arabian oil company because of harsh sanctions in place against Iran in the energy field. Furthermore, a suspicion of Hizbollah involvement in the attack was also investigated, and several Lebanese employees of Aramco were arrested and interrogated.

Conclusion

Iran's developed and developing cyberspace warfare capabilities should be a source of concern to Israel and, of course, the United States, as well as other Western nations. Because of the audacity demonstrated by the attempt on the life of the Saudi Arabian Ambassador to the United States,

American experts feel that Iran's intentions and capabilities in daring to attack critical infrastructures in the United States should not be dismissed. Like the rest of the world, one may assume that Iran too – victim of one of the most destructive cyberspace attacks ever – has learned the lessons of Stuxnet and understands the destructive potential inherent in the development of an offensive tool that could damage industrial control systems, thereby causing physical destruction.

The development of the Iranian strategy and the subsequent force buildup processes indicates systematic preparations and organization with a view to becoming a major cyberspace warfare player. Experts report constant progress in Iran's cyberspace capabilities and operations. Following reports of the cyber attack on the American financial institutions attributed to Iran, one such expert stated, "[Iran's cyberspace program] is similar to the nuclear program: it isn't particularly sophisticated but it moves forward every year."[66] It would be a mistake not to take Iranian technological capabilities seriously. The country's science infrastructure is highly developed and there is a great deal of skilled manpower. One must therefore assume that before too long Iran will represent a significant threat in this area on the global level.

This assessment was further reinforced by the attack on Aramco, after which James A. Lewis, a specialist on cyberspace security, said that Iran was quicker in developing offensive capabilities and more daring in their use than anyone expected.[67] Usually, any activity that is exposed is no more than the tip of the iceberg of concealed activity. Furthermore, Iran's growing defensive sophistication requires interested parties to prepare to operate in an environment of isolated networks or an Iranian network isolated from the World Wide Web. Although the challenge of establishing such a network and achieving total isolation is enormous, such activity is also discernible. This defensive doctrine will represent a very tough challenge indeed for anyone interested in conducting activity in Iranian cyberspace.

The actions attributed to Iran as described above lead to several insights. Iran's attempts to secure SSL permissions indicate work against large groups of citizens rather than focused targets, such as nations or companies and organizations; they are apparently aimed at identifying and monitoring domestic targets. Nevertheless, the cumulative experience gained from such actions will also enable activity against more focused

targets, such as nations and organizations. At the same time, although the detected activity indicates a certain degree of organization and systematic planning, it seems that Iran has yet to cross the threshold into the most sophisticated technological and organizational level. Nevertheless, the country's motivation, force buildup, and technological capabilities will enable it to make very rapid strides in that direction.

The attack on Aramco elicits further conclusions, the first being the fact that conventional defenses against internet threats are not enough. Most experts assume that the company had invested in protection against internet threats. The destructive virus was not discovered by virus protection systems and seems to have been inserted by a company insider possessing the appropriate permission. Current standard protective systems are not built to supply protection against focused threats (APT) and unknown malicious codes (Zero Date and others). Therefore, there is a growing need to develop tools capable of offering better protection against such threats. One such direction lies in developing tools based on the identification, blocking, and neutralization of anomalous and undesirable behavior in the computers under attack. Such tools can neutralize threats even after the malicious code has managed to enter the target computer. A second insight concerns the targets of the attack, which was aimed primarily at the mass and indiscriminate destruction of data in the tens of thousands of computers belonging to the Saudi Arabian oil company, rather than at intelligence gathering. If intelligence gathering in cyberspace may be considered legitimate in some cases, Iranian mass destruction of a civilian target is a sign that Iran is transitioning to retaliation. This should worry those in charge of defense in many nations. Leon Panetta's statement about the need to settle accounts with those behind the attack is one such illustration.[68] But of course actions will speak louder than words.

As the victim of one of the world's most destructive cyberspace attacks, one may assume that Iran fully understands the potential inherent in this realm, and accordingly will work to develop similar capabilities of its own. In that case, the systematic force construction described in this article will very quickly turn Iran into a significant player on the cyberspace battlefield; this will include attacking critical infrastructures in hostile nations, such as the United States and Israel, while creating maximum separation in the event of exposure of such activity. Iran uses so-called civilian hacker communities to try to create a distance between cyber activities and the

regime and official Iranian organizations. A similar approach is adopted elsewhere in the world, e.g. China and Russia, allowing those nations to deny responsibility and lay the blame at civilian doors. Therefore the major challenge of connecting Iran to cyberspace offensives will continue.

Iran's focus of cyberspace activity on Israel and other Western countries requires designated defensive responses. All the countries in question need an updated doctrine on cyberspace defense and protection. The attackers' sophistication necessitates intelligence-based defense activity in addition to generic protections. Therefore, and in light of Iran's development processes, Israel must place Iranian cyberspace high on its list of intelligence priorities, preempting and foiling offenses before they can be carried out. In a way comparable to the Iranian nuclear program, the challenge is not Israel's alone but faces many nations in the West, as well as the Gulf states, as evidenced by the attack on Aramco. Hence, international cooperation of the widest scope possible should be initiated toward intelligence and preemption of Iranian cyberspace activity.

At the same time, Israel must continue to build an effective defensive response focused on three relevant national layers of cyberspace. The first is security organizations, which constantly need to test exposure to Iranian cyberspace capabilities and ensure they are not succeeding in damaging the critical capabilities of the defense establishment. The second concerns the network of critical infrastructures guided by the Information Security Authority by virtue of an Israeli government decision. Here too, the challenge requires constant activity, especially in terms of understanding the threat, adapting the response to it, and sharing information among the various institutions. Finally, one must not dismiss Iran's capabilities and possible attempts to damage non-governmental commerce and industry. Private sector commercial and industrial corporations usually take steps primarily to safeguard their data assets. It is hard to demand that they protect themselves against the possibility of a cyberspace attack from a foreign nation such as Iran. Hence the critical role of the recently established National Cyberspace Staff as an integrating entity capable of promoting processes of regulation, information sharing, and intelligence on the basis of the evolving map of threats.

Notes

1 Art Keller, "The Great Persian Firewall, "*Foreign Policy,* September 2012, p.28, http://www.foreignpolicy.com/articles/2012/09/28/Iran_firewall_google?page=full.
2 Khamenei's statement announcing the establishment of the council on his official website, http://farsi.khamenei.ir/message-content?id=19225.
3 Ilan Berman, "The Iranian Cyber Threat to the U.S. Homeland," Statement before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence, April 26, 2012, pp. 1-3, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Berman.pdf.
4 CBS News, "Iran Confirms Stuxnet Worm Halted Centrifuges," November 29, 2010, http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.
5 Kevin McCaney, "Iran Building a Private, Isolated Internet, but Can it Shut out the World?" *GCN*, April 10, 2012, http://gcn.com/articles/2012/04/10/iran-building-separate-isolated-internet.aspx.
6 Agence France Presse, "Iran Denies has Plan to Cut Internet Access," *AFP*, April 10, 2012, http://www.google.com/hostednews/afp/article/ALeqM5h4e57x6CYbsavza1PeDuQP7Bf9Vg.
7 Amir Taheri, "Iran will Launch its National Internet Next Week but not for the Reasons you Might Think," September 20, 2012, http://www.opednews.com/articles/Iran-will-launch-its-natio-by-Amir-Taheri-120919-83.html.
8 Brian Ross, "What Will Happen to the US If Israel Attacks Iran?" *ABC News*, March 5, 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id1584852.
9 Berman, "The Iranian Cyber Threat to the U.S. Homeland," p. 4.
10 Reza Marashi, "The Islamic Republic's Emerging Cyber War," National Iranian American Council, April 30, 2011, http://www.niacouncil.org/site/News2?page=NewsArticle&id=7318.
11 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.
12 J. P. Patterson and M. N. Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, Master's Thesis (Monterey, CA: Naval Postgraduate School, 2005), pp. 17-22, www.fas.org/irp/eprint/cno-iran.pdf.
13 Sharif University website: http://www.sharif.ir/web/en.
14 Institute website: http://www.aictc.com/web/content/main.
15 Institute website: http://acri.sharif.ir/en/Default.asp.
16 Advanced course descriptions: http://ceit.aut.ac.ir/autcms/courses/courseOfferingView.htm?level=M.Sc&depurl=computer-engineering&lang=en&cid=70317.

17 The data security lab website: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3350532&depurl=computer-engineering&lang=en&cid=147776.
18 The secure systems analysis lab website: http://ceit.aut.ac.ir/autcms/labs/verticalPagesAjax/labHome.htm?id=3369580&depurl=computer-engineering&lang=en&cid=147732.
19 Patterson and Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, pp. 29-35.
20 For more on the center's activity in information security, see http://www.itrc.ac.ir/itrc-secure-en.php.
21 Reference to investments in information technologies at the Technological Cooperation Office website, http://citc.ir/newpages/page27.aspx?lang=Fa.
22 Iran Watch, "The Wisconsin Project on Nuclear Arms Control," January 3, 2011, http://www.iranwatch.org/suspect/records/technology-cooperation-office.htm.
23 The list of companies at Pardis Technology Park is available at http://www.techpark.ir/?/content/142.
24 Guilan Science and Technology Park website: http://www.gstp.ir/modules.php?name=Content&pa=showpage&pid=16.
25 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.
26 Marashi, "The Islamic Republic's Emerging Cyber War." Informational literature presenting the Separ technology and indicating the link between the regime and the technology's development may be found at http://www.iranascience.com/1-home/newsletters/21-Web%20Filters.pdf.
27 OpenNet Initiative, *Internet Filtering in Iran*, June 16, 2009, http://opennet.net/research/profiles/iran.
28 McCaney, "Iran Building a Private, Isolated Internet."
29 Robert Tait, "Iranian State Goes Offline to Dodge Cyber-Attacks," *The Telegraph*, August 5, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html.
30 Cyrus Farivar, "Security Researcher Unearths Plans for Iran's Halal Internet," *Ars Technica*, April 17, 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/.
31 Tait, "Iranian State Goes Offline to Dodge Cyber-Attacks."
32 Ali Akbar Dareini and Brian Murphy, "Iran Internet Control: Tehran Tightens Grip on Web," *Huffington Post*, April 16, 2012, http://www.huffingtonpost.com/2012/04/16/iran-internet-control_n_1429092.html?ref=world.
33 Emily Alpert and Ramin Mostaghim, "Iran's Supreme Leader Calls for New Internet Oversight Council," *Los Angeles Times,* March 7, 2012, http://

latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html.

34 "Structure of Iran's Cyber Warfare," *BBC Persian*, p. 1, http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.

35 "Iran is Formulating Strategic Cyber Defense Plan: Official," *Tehran Times*, June 15, 2012, http://tehrantimes.com/politics/98761-iran-is-formulating-strategic-cyber-defense-plan-official.

36 The center's structure and functions are described on its official website: http://www.certcc.ir/index.php?newlang=eng.

37 "Structure of Iran's Cyber Warfare", pp. 4-5.

38 "Iran to Crack Down on Web Censor-Beating Software," *Hürriyet Daily News*, September 22, 2012. http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374.

39 "Structure of Iran's Cyber Warfare," p. 4.

40 In January 2012 the regime passed a set of laws for monitoring and surveillance of web surfers at internet cafes throughout the country. These laws allow FETA to create a user log of all temporary surfers in the country and monitor anti-regime activities in cyberspace. Farnaz Fassihi, "Iran Mounts New Web Crackdown," *Wall Street Journal*, January 6, 2012, http://online.wsj.com/article/SB10001424052970203513604577142713916386248.html.

41 Berman, "The Iranian Cyber Threat to the U.S. Homeland," p. 4.

42 Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," *Defense Tech*, September 23, 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment.

43 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.

44 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," A Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies. April 26, 2012, p. 5, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf.

45 Scott Peterson, "Iran's Cyber Prowess: Could it Really have Cracked Drone Codes?" *Christian Science Monitor*, April 24, 2012, http://www.csmonitor.com/World/Middle-East/2012/0424/Iran-s-cyber-prowess-Could-it-really-have-cracked-drone-codes.

46 Cilluffo, "The Iranian Cyber Threat to the United States," p. 5.

47 Patterson and Smith, *Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran*, pp. 44-49.

48 Iftach Ian Amit, "Cyber [Crime|War]," paper presented at DEFCON 18 Conference, July 31, 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Amit/DEFCON-18-Amit-Cyber-Crime-WP.pdf.

49 Khashayar Nouri, "Cyber Wars in Iran," *Institute for War & Peace Reporting,* July 23, 2010, http://iwpr.net/report-news/cyber-wars-iran.

50 Golnaz Esfandiari, "Basij Members Trained to Conquer Virtual World," *Payvand Iran News*, August 21, 2010, http://www.payvand.com/news/10/aug/1206.html.

51 Jeffrey Carr, "Iran's Paramilitary Militia is Recruiting Hackers," *Forbes,* January 12, 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/12/irans-paramilitary-militia-is-recruiting-hackers/.

52 Bob Beauprez, "Iranian Cyber-Attack Plot against U.S. Exposed in Mexico," *Townhall*, December 13, 2011, http://finance.townhall.com/columnists/bobbeauprez/2011/12/13/iranian_cyber attack_plot_against_us_exposed_in_mexico/page/full/.

53 SSL is a protocol for security communications on the internet, making sure that the server a client is contacting is in fact the right server, while encrypting the information between the browser and the server. SSL keys can be purchased from authorized providers. The theft of keys would allow the thief (with control of the network's infrastructure) to divert surfers to counterfeit websites masquerading as legal sites and thereby access confidential information about the user.

54 Report issued by Comodo Ltd., March 13, 2011, http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html.

55 Eva Galperin, Seth Schoen, and Peter Eckersley, "A Post Mortem on the Iranian DigiNotar Attack," *Electronic Frontier Foundation,* September 13, 2011, https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack.

56 Fox-It, Interim Report, "DigiNotar Certificate Authority Breach 'Operation Black Tulip,'" September 5, 2011.

57 Toby Sterling, "Iran Involvement Suspected in DigiNotar Security Firm Hacking," *HuffPost Tech*, September 5, 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html.

58 Gerry Smith, "Cyber Attacks Against US Banks Sponsored by Iran, Lieberman Says," *Huffington Post,* September 9, 2012.

59 The FS-ISAC is an organization whose role is to analyze and share information among financial institutions about threats to critical financial services in the United States.

60 Jaikumar Vijayan, "U.S. Banks on High Alert against Cyber Attacks," *Computerworld*, September 20, 2012, http://www.computerworld.com/s/article/print/9231515/U.S._banks_on_high_alert_against_cyber ttacks.

61 Jim Finkle, "Exclusive: Insiders Suspected in Saudi Cyber-Attack," *Reuters*, September 7, 2012, http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907.

62 Kelly Jackson Higgins, "Shamoon Code 'Amateur' but Effective," *Dark Reading*, September 11, 2012, http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240007179/shamoon-code-amateur-but-effective.html; Nicole Perlroth, "Cyber Attack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyber attack-on-saudi-oil-firm-disquiets-us.html?_r=1&adxnnl=1&pagewanted=all&adxnnlx=1351084069-1i53F0BCczNEGcP8ut3n4A&.

63 Associated Press, "Panetta Hints Iran behind Gulf Cyber attacks," *CBS News*, October 12, 2012, http://www.cbsnews.com/8301-202_162-57531088/panetta-hints-iran-behind-gulf-cyber attacks.

64 Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" Blogspot, August 27, 2012, http://jeffreycarr.blogspot.co.uk/2012/08/whos-responsible-for-saudi-aramco.html.

65 Global Research & Analysis Team, "Shamoon the Wiper – Copycats at Work," *Kaspersky Lab Expert*, August 16, 2012, https://www.securelist.com/en/blog?print_mode=1&weblogid=208193786.

66 Reuters, "Iranian Hackers Attacked Three Largest U.S. Banks as Part of Cyber Campaign: Sources," September 21, 2012, http://news.nationalpost.com/2012/09/21/iranian-hackers-attacked-three-largest-u-s-banks-as-part-of-cyber-campaign-sources.

67 Perlroth, "Cyber Attack on Saudi Firm, U.S. Sees Iran Firing Back."

68 Associated Press, "Panetta Hints Iran behind Gulf Cyber Attacks."

The Growing Power of the Indian Navy: Westward Bound

Yuval Zur, Tamir Magal, and Nadav Kedem

Introduction

India is a rapidly developing nation enjoying impressive economic growth.[1] Its influence in the international arena has increased over the years and is expected to continue to rise.[2] Alongside this expanding influence, the country is experiencing a burgeoning sense of identity as an international power, and there is a growing perception in India that its national interests extend far beyond its sovereign borders. Hence the country's efforts to protect those interests through maritime diplomacy and, in the same context, project its maritime power in relevant regions. In other words, India is interested in expanding its capabilities to protect its vital interests, by expanding its presence and gaining sustained sea control and maritime awareness beyond its territorial boundaries.

This article reviews India's gradual rise to the status of international power and its growing interest in the "expanded neighborhood,"[3] with a focus on the western section of that "neighborhood." This comprises, first and foremost, the maritime region west of India through the Strait of Hormuz in the north and the Gulf of Aden and Horn of Africa in the south, and also includes the Persian Gulf, the Red Sea, and the East African coast. The terms "power projection," "sea power," and "blue-water navy" will be explained through a review of the Indian Navy's development and its

Admiral (ret.) Yuval Zur was assistant commander of the Israeli Navy. After his retirement from the IDF he served as assistant head of the Israel Atomic Energy Commission. He is currently the Principal Maritime Strategic Chair at the department of Maritime Civilizations at the University of Haifa. Tamir Magal is a research assistant at INSS. Nadav Kedem, a former Neubauer research fellow at INSS, is a doctoral student in political science at the University of Haifa.

potential deployment west of India. Lastly, and in view of these trends, the article examines the implications of that developing potential for Israel.

India as a Rising Power

Since gaining independence, India has seen itself as a key player in the international arena and has acted independently, even provocatively, toward the US and the Soviet Union. However, its economic and military strength have not been commensurate with its global aspirations. The end of the Cold War brought about a substantial change in India's geopolitical and strategic environment: the Soviet Union, India's biggest supporter, collapsed; its great regional adversary, China, had already laid the groundwork for its own growing power; the road to improved relations with the US opened up; and the Indian economy underwent extensive domestic reform and began to grow at an impressive rate. India's scope of possibilities broadened in light of its expanding economic power. Further potential for developing spheres of influence emerged in the wake of the Soviet Union's collapse and limited American ability to establish its presence in different areas of conflict across the globe.

Moreover, India's economic development necessitated an increased supply of raw materials and finished goods. Accordingly, India, poor in natural resources and possessing a limited industrial infrastructure, began to take an interest in international sea lines of communication (SLOC)[4] so as to ensure a supply of those resources. Finally, the ascent of China, India's "natural adversary," led to revised strategic thinking that emphasized the need for enhanced Indian power. In other words, India felt it was important (and not unrealistic) to challenge China in regions that are deemed vital for its national security.

It is worth noting that China places great importance on the "String of Pearls," key SLOCs extending from the Chinese mainland to East Africa, and invests great effort in securing its influence in those regions. The "String of Pearls" routes surround India and constitute part of China's strategy for securing its eminence in the Indian Ocean. Not surprisingly, this strategy increases Indian fears of exclusion from this region.

The changes underway in India are slow and long term. Gross domestic product (GDP) is still significantly lower (when adjusted for exchange rate) than those of Germany, the UK, and France (all considerably smaller countries). India's industrial base remains limited, infrastructures are inadequate, and the country faces internal challenges of Herculean proportions. To a large extent India's national security objectives and their

derivate strategies in the post-Cold War era are still evolving. Nevertheless, there is a consistent and ongoing process of developing an identity of an important regional power, with interests and influence in regions that are not necessarily adjacent to its borders. This process continues under varying ruling coalitions, with no apparent dispute over this general direction among the Indian public and its decision makers.

India's Sphere of Influence Defined

In a 2007 speech, former Secretary of the Indian Ministry of Defense[5] Shekhar Dutt defined the sphere of influence that India aspires to:

> Given the size of the country and its role in the comity of nations, our security concerns are not limited to our immediate neighborhood...India's area of security interest extends beyond the confines of the conventional geographical definition of South Asia...India's security environment extends from the Persian Gulf to the Straits of Malacca across the Indian Ocean, including the Central Asian region in the North West, China in the North East and South East Asia.[6]

In addition to this agreed definition, there are Indian leaders who extend this region further to the west and south. For instance, according to former Foreign Minister Yashwant Sinha, "extended neighborhood" for India "stretches from the Suez Canal to the South China Sea and includes within it West Asia, the Gulf, Central Asia, South East Asia, East Asia, the Asia Pacific and the Indian Ocean Region."[7]

India's primary interests in these regions are to defend its exclusive economic zone (EEZ), to secure India's access to SLOCs across the Arabian Sea, and to solidify its status in these regions vis-à-vis China. In this context it is important to note that the Arabian Sea serves as a junction for maritime routes that run through the Suez Canal and the Red Sea, as well as the Persian Gulf. Former Chief of the Indian Navy, Admiral Sureesh Mehta, said:

> Within the overall national and defense framework, our primary maritime military interest is to ensure national security, provide insulation from external interference, so that the vital tasks of fostering economic growth and undertaking developmental activities can take place in a secure environment. Consequently, India's maritime military strategy is

> underpinned on "the freedom to use the seas" for our national purposes, under all circumstances.[8]

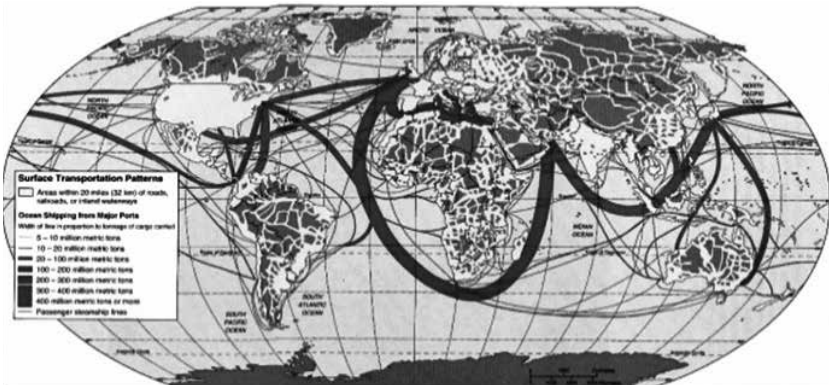
Other interests can also be noted, including the conspicuous example of the "special" relationship between India and the Persian Gulf region. In fact, India's commercial and cultural ties with the Gulf region date back to ancient times. Those relations deviated somewhat from their path following India's independence, but the basic underlying structure of mutual interests appears to have contributed to their recent flourishing. India also enjoys the constant flow of high revenues from Indian foreign workers in the Gulf. Moreover, a sort of "natural" reciprocal linkage seems to be evolving, with the Gulf states needing Indian technology, know-how, and skills, and India needing energy and investments from the Gulf. From India's point of view, this is a "natural" alliance that is stable and convenient for all concerned.

To a large extent, the Gulf region serves as a natural hinterland for India in terms of commerce and the supply of resources. The region's importance has grown as a result of India's growing thirst for natural resources. The need to expand and diversify energy sources (different types of energy sources and different countries of origin) is vital for India. To be sure, India is not alone in its craving for the Gulf's energy resources. Other powers, including India's arch-rival China, are equally thirsty for resources. The US withdrawal from Iraq and anticipated withdrawal from Afghanistan are fueling apprehensions over a possible power vacuum, due to weakened American influence in the region. The growing potential for oil production in East African countries, as well as active oil fields in Sudan and Egypt, further underlines the need to secure access and trade routes to energy sources in the region.

The map below illustrates the course of Indian SLOCs that run adjacent to the Horn of Africa and the Arabian Peninsula, as well as the southern coasts of Iran and the Strait of Hormuz; clearly, India has an interest in defending these routes. Moreover, the various dangers lurking along these lanes are not merely theoretical. Even today, pirates operating close to the Somali coast and in the Gulf of Oman attack Indian merchant vessels. Such piracy and international maritime terrorism are especially worrisome in light of East Africa's rapidly increasing capacity for oil production.

In many respects, the United States Navy currently supplies a "public good" that ensures the free flow of trade and resources from the region.

World Transportation Patterns



However, even the US Navy has limited capability. Furthermore, American interests are not always compatible with those of other countries, and any cooperation with other navies is subject to American limitations. India is concerned that it will not be able to continue relying wholly and exclusively on the US Navy in this regard. Friction between India and the US was already apparent in 2003, against the backdrop of an American initiative for joint maritime cooperation within the framework of the Proliferation Security Initiative.[9]

Iran's unique role as India's provider of an overland route to Central Asia is important in this context,[10] due to India's inability to access this region via its adversaries China and Pakistan (who are themselves allies). India attributes significant importance to developing ties with central Asian countries. Those countries are perceived inter alia as an important source of natural resources, but also as potential threats for national security (through terrorism). The ambitious project of developing the Iranian port of Chah Bahar is a case in point. India contributed substantially to the construction of this port, which is meant to serve as an Indian passageway to central Asia, and is currently involved in laying a railway between Chah Bahar and Afghanistan. Concurrently, the generous financial assistance extended[11] to Afghanistan, second in scope only to US assistance, is only one of many examples attesting to India's desire to keep a watchful eye on central Asian countries. Iranian ties with extremist Sunni groups in Afghanistan and Pakistan can also assist India in restraining those groups. In fact, India needs Iran to serve as a kind of counterbalance against its

adversary, Pakistan. India also has an interest in using its connections with Gulf states to prevent overly close relations between the two Sunni allies, Saudi Arabia and Pakistan.

Power Projection and Sea Power

The term "power projection" refers to a country's ability to exercise political, economic, strategic, and military power in order to advance its strategic objectives.[12] Among other things, the military component of power projection also relates to an ability to employ military force for a sustained period of time, far from its territorial boundaries. However, the ability to execute a pinpointed attack on distant targets does not fully constitute power projection, as it lacks the element of a sustained period.

Traditionally, power projection relied on "sea power," defined as the ability to exert influence "at sea and from the sea."[13] In addition to military components, such power includes many other elements, such as the merchant fleet, fishing fleet, maritime industries, ship building, and repair. Sea power is relative, not absolute, and is important at times of both peace and war.

A central component of military sea power is large surface vessels.[14] These vessels have the capacity to maintain their presence at sea for extended periods at longer ranges form their home ports, and possess greater firepower in comparison with smaller combat ships and military aircraft. Most power projection operations in recent decades have involved significant use of sea power (Iraq, Libya, Afghanistan, Somalia, Falklands).[15]

Naval operations at high seas are conducted in the framework of battle groups/ task forces. These groups include a number of ships with differing functions (anti-aircraft, anti-submarine, anti-missile, minesweeping, missile launching), which complement and defend each other. Historically, battle groups evolved around aircraft carriers during World War II; even today battle groups are built around large command ships such as aircraft carriers or amphibious assault ships (LPD/LDH). With a displacement of 40,000 to 60,000 tons, these ships provide the command and logistical basis of the battle group, while also capable of employing fighter aircraft (in the case of aircraft carriers). The ability to deploy aircraft at sea combines the advantages of the two different operational capabilities: the speed and flexible response of combat aircraft, together with the long range and endurance of ships. Nevertheless, while aircraft carriers and amphibious

assault ships enable performance of a variety of power projection missions, some of those missions, such as defending trade routes or fighting piracy, do not necessarily require the use of these types of vessels. Today, only 13 countries operate aircraft carriers, with India being one of them.[16]

The Development of the Indian Navy

In its first decades the Indian Navy was composed mainly of small ships (under 3,000 tons), and for the most part carried out missions aimed at defending Indian littoral waters. However, as early as 1957 the Navy purchased a "light" aircraft carrier, the *Vikrant,* from Britain. This model, which was built during World War II, was smaller than standard aircraft carriers (20,000 as compared to 40,000 tons), and enabled the deployment of sort-range combat aircraft. The *Vikrant* led a battle group of three ships, based in the Andaman Islands. This group participated in the India-Pakistan war of 1971, when its combat aircraft attacked remote ports in Bangladesh. The war led to a recognition of the Indian Navy's operational shortcomings, as well as an understanding of the need to build a "blue-water navy," which would be able to operate across open oceans.

In the early 1980s India began purchasing destroyers and missile-carrying frigates, along with smaller ships designated for operations in territorial waters. The ships were constructed mainly by foreign shipyards in Britain and Russia, while a local infrastructure for the construction of large ships was under development. Even today India requires significant technological assistance in incorporating various weapons systems aboard its ships.

By the late 1980s, the Indian Navy included five destroyers, three frigates, four corvettes, and six submarines equipped with cruise missiles. This was in addition to two aircraft carriers: the veteran *Vikrant*, which was decommissioned in 1997, and another light aircraft carrier (*Viraat)*, purchased in 1986 after 17 years of service in the Royal Navy. Early in the twenty-first beginning century, the Indian Navy boasted one aircraft carrier, eight destroyers (7,000 tons), nine frigates (4,000-5,000 tons), eight corvettes (2,500-3,000 tons), and ten cruise missile-carrying submarines. These ships are equipped with missile for ranges of 200-300 kilometers, including Indian-made cruise missiles.

Table 1depicts the size of the Indian fleet at the start of the 21st century, and compares the number of its platforms with those of other navies during

that period.[17] From the table we can conclude that the Indian Navy, although not in the same league as veteran powers like France and Britain, is engaged in a rapid process of developing power projection capabilities in a number of fields. Its progress during these years is significant in comparison with small regional navies, such as that of Pakistan. Other comparative studies of world navies classified the Indian Navy, together with China, one level below the European powers (Britain and France), but above regional navies such as those of South Africa and Israel.[18]

Table 1. Comparison of Navies

	India	Britain	France	China	Pakistan
Aircraft carriers	1	3	1		
LPD class ships		3	6		
Ballistic submarines		4	4	2	
Cruise missile submarines	10	12	8	9	11
Destroyers	8	11	14	21	
Frigates	9	20	24	12	6
Corvettes	8			28	

Current Projects

In the past decade the Indian Navy has overseen a series of projects of building new vessels that will increase its operational capability as a blue-water navy. These projects, mostly conducted by local shipyards, are well advanced, with some on the verge of completion. However, all of them include integration of weapon systems from foreign sources. The following section surveys these projects and their progress, divided according to aircraft carriers, combat vessels, and submarines.[19]

Aircraft Carriers

In 2004 India began building two new, larger aircraft carriers. The first contract, between India and Russia, included the sale of a "standard"[20] Kiev class Russian aircraft carrier, which was launched in 1987 but decommissioned in 1996. The deal included a full overhaul of the ship's systems and the addition of a second runway. Disputes over price held up the transaction until an agreement was concluded in March 2010 ($2.35

billion). In June 2012 the aircraft carrier *Vikramaditva* began a number of sea trials prior to delivery to the Indian Navy.[21] The ship, 283 meters in length with a displacement of 45,500 tons, will employ standard MiG-29K aircrafts as well as Ka-31 naval helicopters.

The second contract, for building a locally constructed aircraft carrier, the *Vikrant*, was signed with the Cochin shipyard in 2004. In 2006 the final structure of the carrier was determined, i.e., a standard aircraft carrier measuring 260 meters in length with a displacement of 40,000 tons. In December 2011 the completed hull of the carrier was floated out of dry dock, signifying 40 percent completion of the project, with sea trials expected at the end of 2014 and entry into active service in 2015. The carrier is designed to carry standard MiG-29Ks, Indian Tejas aircraft, and Ka-31 naval helicopters.

Additionally, in June 2007 an amphibious LPD class ship, with a displacement of 16,500 tons, the *Jalashwa,* entered service with the Indian Navy. The ship, which carries a number of landing craft and Sea King transport helicopters, was procured from US Navy surplus and enables the deployment of amphibious forces away form India's littoral waters.

Combat Vessels

In order to increase the number of large combat vessels at its disposal, the Indian Navy has for the past decade been directing a number of projects for the construction of new destroyers and frigates, mainly in collaboration with local shipyards. These projects include:

Project 15A – for the construction of three Kolkata class destroyers, with a displacement of 7,000 tons each, in association with the Magazon shipyard in Mumbai. These destroyers are equipped with Indian-made BrahMos cruise missiles and Israeli-made Barak surface to air (SAM) missiles. The first ship of this type entered service in 2011; the remaining ships are in advanced stages of construction.

Project 17 – for the construction of three Shivalik class frigates, with a displacement of 5,300 tons each, in association with the Magazon shipyard in Mumbai. These frigates are equipped with Russian SS-N-27 Club-N cruise missiles. The project was completed with the entry of the last frigate into service in 2010.

Talawar project – for the construction of three Talawar class frigates with a displacement of 4,000 tons each, in association with the Russian

Yantar shipyard in Kaliningrad. These frigates will join the three frigates of this class already in service with the Indian Navy. The ships are equipped with BrahMos and Club-N cruise missiles. The first ship entered service in 2012 and the remainder are in advanced stages of construction.[22]

Project 28 – for the construction of up to 12 missile-carrying corvettes, with a displacement of 2,500 tons each, in association with Calcutta shipyards. These ships will be equipped with Club-N missiles and Israeli Barak-8 SAM missiles. The first four ships are in advanced stages of construction, with entry into service expected in 2012.

Most of these projects involve Israel Aerospace Industries (IAI), which supplies the Indian shipyards with radar systems and the Barak-8 missile for anti-aircraft and anti-missile defense.

Submarines

Since 2004, the Indian Navy has overseen a project for a locally built nuclear powered ballistic missile submarine (SSBN). The submarine, named the *Arihant,* has been undergoing sea trials since 2010 and should be declared operational in 2012. The development of the submarine's missile launching capability is underway alongside India's success in completing development of an intercontinental variant of the *Agni* missile.[23] Additionally, in June 2012 the navy completed the upgrade of ten kilo class cruise missile-carrying submarines, which have been in service since the 1990s. These submarines were overhauled, and equipped with modern Club-S cruise missiles.[24] The navy is also leasing a Russian nuclear-powered Akula class attack submarine, which likewise carries cruise missiles.

At the current rate of progress, therefore, the above projects are likely to be completed in 2015. By then, the Indian Navy will comprise a sufficient quantity of large combat vessels for up to three battle groups. Following completion of the *Vikramaditva* aircraft carrier, the navy will include two active aircraft carriers as well as an amphibious LPD class vessel. This quantity of flag ships will make it possible to construct two to three battle groups. Given India's need to divide its navy between an eastern command and a western command, the creation of three battle groups will enable greater freedom of action in deploying the navy in the Gulf of Aden. By contrast, the establishment of only two battle groups would reduce the navy's scope of action to the eastern Arabian Sea.

Indian Navy Power Projection Mission

Over the past decade the Indian Navy, despite its limited size, has worked persistently to project its power and capabilities to the furthest edges of its delineated "expanded neighborhood." These efforts included activities from the South China Sea to the eastern Mediterranean, and specifically within the western part of the Indian Ocean.[25]

A key example of these efforts is the protection of freedom of navigation and maritime security. As part of this mission, India is already maintaining a permanent presence in two key areas in the Arabian Sea: since 2008 there has been a permanent combat vessel stationed in the Gulf of Aden to protect against pirate attacks on Indian merchant vessels. In addition, reconnaissance planes and combat vessels are permanently stationed near the Seychelles, aimed at monitoring the islands' economic zone, as well as maritime traffic along the East African coast. A further increase in the size of Indian naval forces would likely lead to the permanent presence of an Indian battle group in the Gulf of Aden and increased Indian involvement in the struggle against piracy.[26]

Furthermore, India is demonstrating its presence by "showing the flag" in new regions. Since the beginning of the 21st century, a flotilla of three or four Indian vessels has made annual visits to the Gulf of Oman, the Persian Gulf, the Red Sea, and on occasion the Mediterranean. The flotilla enters various ports in the region and conducts joint exercises with local navies,[27] further substantiating and deepening relations with the regional nations. With the introduction into service of a second aircraft carrier and further growth in the size of the navy, such visits are likely to develop into the continuous presence of an Indian battle group in the Gulf of Oman.

Another mission of the navy is to protect Indian citizens in foreign countries and evacuate foreign citizens from countries of conflict. India's ability in this area was illustrated in July 2006, when four Indian warships evacuated foreign citizens from Lebanon at the height of clashes between Israel and Hizbollah.[28] Future Indian action could even include involvement and assistance in humanitarian crises, as instanced in India's involvement in the 2004 tsunami.[29]

Additionally, in the past the Indian Navy executed amphibious operations deploying significant ground forces in distant countries to confront revolutions and rebellions against local governments.[30] Such missions, which were previously limited to countries with India's

traditional zone of influence, could signify a new stage in India's power projection capabilities – military involvement in more remote locations where India maintains vital commercial and energy interests.

In light of its interest in accessing Central Asia, India might feel the need to warn other players against attacking Chah Bahar port in Iran, a theoretical situation that could result in a confrontation with a third party.

India-Israel Naval Relations and their Potential Development

The relationship between India and Israel has developed rapidly since the establishment of diplomatic relations in 1992.[31] In commercial terms Israel is considered an "insular state," with 98 percent of its foreign trade conducted via maritime routes.[32] Currently, Israel's major trade routes pass through the Mediterranean Sea; however in the past the Red Sea was also an important route and might be reconsidered as such in the future. As an insular state, Israel needs to safeguard its SLOCs and develop economic and security ties overseas; hence there is considerable strategic logic in further developing Israeli-Indian cooperation in the maritime arena. Beyond their extensive trade relations, there are large scale Israeli arms sales to India, as well as enhanced intelligence collaboration. However, these mutual relationships have thus far been restricted, in part by India's extensive relations with Iran and Arab nations and its large Muslim minority.

These limitations have resulted in relatively minor military cooperation between the two countries, with India preferring to maintain a very low public profile on these relationships (mainly in political and security contexts). Still, there is ongoing contact between the Indian and Israeli navies, including visits of Indian ships to Israeli ports,[33] as well as reciprocal visits by senior officers of both countries.[34] These visits fulfill the role of "showing the flag" and demonstrating sustained presence, which signifies national interests and key foreign policy objectives.

However, the scope of these visits exceeds the need for securing trade routes and signifies a commonality of interests regarding the growing challenges to global security in the maritime arena. Globalization has magnified a variety of such threats, including maritime terrorism, piracy, proliferation of weapons of mass destruction, and the smuggling of weapons, drugs, or illegal immigrants. Confronting these threats necessitates "maritime domain awareness" (MDA)[35] and induces the

incentive for technological and operational collaboration between the navies.

Technological cooperation between Israel and India developed in the 1990s in response to the Israeli defense industry's need to find new markets, which coincided with India's need for advanced military technology. The crisis in the Russian defense industry, combined with American unwillingness to sell arms, led India to seek alternative sources for modern technology. The Israeli defense industry identified correctly the potential of the Indian market, particularly India's need for modern maritime technology.

This technological cooperation was based on mutual interests in both navies: the Indian Navy assured itself high quality projects, advanced technology, and system specifications suited to the modern naval arena. The Israeli Navy, through its defense industries, would spearhead development and equip itself with systems that – barring Indian collaboration – budget restrictions would otherwise not have permitted (in terms of investment in development and the scope of procurement).

Within the framework of this technological cooperation India equipped its vessels with Barak air defense missiles and on-board radar systems. Additionally, India procured UAVs for maritime patrol missions, as well as Aerostat-borne radar and surveillance systems for coastal defense. Without a doubt, from Israel's point of view, its defense export policy is the key incentive for developing cooperation between the two navies. However, the potential in these relationships is far greater.

Future Directions of Israeli-Indian Maritime Cooperation

One of the challenges facing the Israeli Navy is the difficulty of sustaining operations at long distance from Israeli ports. The Indian Navy could grant Israeli vessels access to its ports, similar to the visits of Indian ships to Israeli ports. In such a way the Israeli Navy can replenish its vessels and extend its operational reach.

Sustained collaboration between the two navies could in the long term lay the foundations for Israeli participation in international maritime enforcement operations. Without taking a stand in this regard, Israeli participation in such operations may yield substantial political gains.

Moreover, higher cooperation between the navies could enable covert operational collaboration. For example, based on existing intelligence

cooperation, Israeli vessels, and in the future perhaps Indian vessels too, might be able to intercept ships that are smuggling weapons to the region. At present, there is little likelihood that India would agree to halt Iranian ships. However, it could offer behind-the-scenes assistance, in terms of intelligence and logistics, which would enable Israeli vessels to intercept suspicious ships. Indeed, it would be ill advised for Israel to rely solely on the US Navy in this regard. Despite its sheer size, even the US Navy has its limitations. Moreover, it is wiser to diversify the sources of intelligence and expand the toolbox at Israel's disposal.

Furthermore, sustained cooperation fosters personal ties between Indian and Israeli officers, which in turn tend to foster and generate new channels of communication. India maintains extensive ties with Persian Gulf states, including Iran and Afghanistan, and closely monitors threats of Islamic terrorism. These may generate a shared interest in an ongoing exchange of valuable information, with appropriate attention to precautionary measures.

It is impossible to ignore the fact that Indian political and geostrategic considerations are liable to restrict the development of such cooperation. Two aspects to bear in mind, among others, are India's preference for maintaining a relatively low profile vis-à-vis the relationship with Israel, and the importance it ascribes to preserving its connection with Iran. Nonetheless, it is not inconceivable for political changes in India and/or other developments to turn higher cooperation between the two nations into a political reality. Ultimately both need each other, and thus cooperation is natural. It is essential for Israel to take an overall view of its relations with India, rather than focusing primarily on the potential for arms export.[36] Arms exports have indeed leveraged relations favorably for Israel. However, they alone are insufficient to realize the broader potential of relations between the countries, particularly between their navies. Accordingly, such cooperation should be viewed as a prime objective that Israel should aspire to realize, in accordance with the developments and opportunities it encounters along the way.

Notes

1 For an extensive review of the rise of India, see Sumit Ganguly and Rahul Mukherji, *India since 1980* (New York: Cambridge University Press, 2011).

2 For a critical review of the rise of India, see Sumit Ganguly, "Think Again: India's Rise," *Foreign Policy*, July 5, 2012.

3 As seen below, "the Indian neighborhood" is a term used in Indian discourse concerning its foreign policy.
4 Sea lines of communication refer to the primary maritime routes between ports, used for trade, logistics, and naval forces.
5 Equivalent to Israel's Director General of the Ministry of Defense.
6 Shekhar Dutt, "Defense, Security, Diplomacy: India's National Interests," February 24, 2007, www.associationdiplomats.org/specialevents. Identical formulation used in the Ministry of Defense, *Annual Report 2006-2007* (New Delhi: Ministry of Defense, 2007).
7 Yashwant Sinha, "12th SAARC Summit and Beyond," February 3, 2004, http://www.outlookindia.com/article.aspx?222849. It is customary in India to refer to the Asian portion of the Middle East as well as part of the Caucasus as West Asia. There is no agreed upon exact definition of this region.
8 Sureesh Mehta, "Freedom to Use the Seas: India's Maritime Military Strategy," Integrated Headquarters, Ministry of Defense (Navy), New Delhi, 2007.
9 The PSI was formulated to prevent maritime transport of weapons of mass destruction and launch weapons such as ballistic missiles.
10 For a review of India's power projection that includes expanded reference to Iran, see David Scott, "India's 'Extended Neighborhood' Concept: Power Projection for a Rising Power," *India Review* 8, no. 2 (2009): 107-43.
11 India itself benefits from assistance from other countries.
12 Dictionary of Military and Associated Terms, US Department of Defense, 2005.
13 A. Mahan, *The Interest of America in Sea-Power, Present and Future* (London: Sampson Low, Marston & Company, 1898).
14 Combat vessels above 3,000 tons DWT.
15 A more current term is "expeditionary forces."
16 The presence of aircraft carriers in any given country's fleet does not necessarily give that country significant maritime power (e.g., Thailand). Aircraft carriers must form part of an overall power projection system.
17 A comparison between fleets is distinct form comparison between navies, which also includes their training and infrastructure. Furthermore, a comparison between platforms does not take into account technological differences in weapon systems installed on them.
18 An accepted classification in this area is the study by Eric Grove, *The Future of Sea Power* (Annapolis: Naval Institute Press, 1990).
19 Information on the projects is taken for the most part from *Jane's Fighting Ships 2011*.
20 Aircraft carriers are classified into three types on the basis of size: "light"' aircraft carriers with a displacement of up to 30,000 tons; "standard" aircraft carriers with a displacement of 40,000-60,000 tons; and "super" aircraft carriers with a displacement in excess of 100,000 tons.

21 Christopher P. Cavas, "Indian Carrier Begins Sea Trials," *Defense News*, June 8, 2012.
22 "Russian-Built Frigate Arrives in India," *RIA Novosti*, June 22, 2012, http://en.rian.ru/world/20120622/174181942.html.
23 Mark Magnier, "India Ballistic Missile Test is a Success," *Los Angeles Times*, April 19, 2012, http://articles.latimes.com/2012/apr/19/world/la-fg-india-missile-test-20120419.
24 V. Radyuhin, "Russia Completes India's Submarine Modernization Program," *The Hindu*, June 23, 2012.
25 Walter C. Ladwig, "India and Military Power Projection: Will the Land of Gandhi Become a Conventional Great Power?" *Asian Survey* 50, no. 6 (2010): 1162-83.
26 Scott, "India's 'Extended Neighborhood' Concept."
27 Joint exercises with Persian Gulf states were conducted in 2002, 2004, 2007, and 2011.
28 Bjarat Rakshak, "Operation Sukoon," http://www.bharat-rakshak.com/NAVY/Galleries/News/Sukoon/.
29 "Operation Madad," *Wikipedia*, http://en.wikipedia.org/wiki/Operation_Madad_%28Indian_Navy%29.
30 Ladwig, "India and Military Power Projection."
31 For an extensive review see P. R. Kumaraswamy, *India's Israel Policy* (New York: Columbia University Press, 2010).
32 See *Ports & Shipping Statistical Yearbook*, http://spa.mot.gov.il/images/PDF/SHNATON/StatisticalYearBook11.pdf.
33 The most recent visits of Indian warships to Israel were in June 2006 and July 2012. See Aluf Benn, "Two Indian Warships Arrive in Haifa for a Friendly Visit," *Haaretz*, June 28, 2006, http://www.haaretz.co.il/misc/1.1116116; and Amir Buhbut, "Against the 'Red Fleet': See the Expanded Missile Boat Exercise," *Walla*, August 1, 2012, http://news.walla.co.il/?w=/551/2554984.
34 For a brief overview of relations between the navies, see http://www.gloria-center.org/2011/12/indo-israeli-defense-cooperation-in-the-twenty-first-century/.
35 Maritime Domain Awareness (MDA) involves an overall understanding of all matters related to the maritime domain, including the interaction of the maritime domain with security, economic, and diplomatic issues.
36 There is currently increasing involvement of numerous Israeli organs, in addition to the Ministry of Defense, in the relationship with India.

Cybercrime: A National Security Issue?

Lior Tabansky

Cyberspace, an offshoot of the development of computer and digital communications technologies, has in recent decades become part and parcel of our lives. Computerization is invaluable in improving and streamlining processes related to work, learning, and entertainment, and it affects virtually every field of human endeavor. Once the internet became commercial in 1988, it quickly turned into a mainstay of cyberspace, offering inexpensive and immediate access to many sources of information, information sharing, joint long distance work, and more.

The implications of cyberspace crime for national security derive from the way technology is used by hostile elements. This article proposes a policy directed examination of the meaning of cyberspace crime and its impact on national security, without focusing on the widespread monetary assessments of the damage caused by cybercrime. It includes a profile of cooperation among criminals, organized crime, and hostile organizations, and discusses the commercialization of cyber reconnaissance and cyber attack capabilities, made possible by ever-developing technologies and the growth of a black market in IT services. Currently, cybercrime is hardly significant beyond the realms of IT risk management and law enforcement. However, this article identifies two separate conditions where cybercrime could become a substantial threat to national security.

Public demand for cyber security rises in proportion to the growing recognition of the menace. Even in the absence of an objective increase in the scope of crime, this demand is not expected to decrease. The state's responsibility to provide security to its citizens cannot stop at the threshold

Lior Tabansky, a former Neubauer research fellow at INSS, is a doctoral student in the Department of Political Science at Tel Aviv University.

of cyberspace, and in this realm too the practical expressions of such responsibility must be defined as part of a democratic political process on a firm factual basis.

The Cybercrime Phenomenon

Computerization allows tasks to be broken down into small units and decentralizes processing; networking allows global access to information and focus on knowledge as a valuable product. Computerized technologies are implemented to change and enhance the efficiency of creative and working processes in every aspect of life, and the world of crime is no exception. The proposed definition of cybercrime is: "The use of cyberspace for illegal ends, while exploiting unique cyberspace features, such as speed and immediacy; remote operation; encryption and obfuscation, making it difficult to identify the operation and the operator."

The debate on cybercrime continues. Over a decade ago, Grabovsky wondered what was new about cybercrime, whether it was not merely an old phenomenon making use of new tools.[1] But most researchers try to analyze cybercrime as a unique phenomenon. Majid Yar categorizes it according to the object targeted: property, people, or the state.[2] Shinder and Cross distinguish between types of crime according to the level of violence involved: violent and potentially violent crime, non-violent crime (drug trade, money laundering), and crime (still) perceived to fall within the white collar category (computer break-ins, theft, and fraud).[3] According to Wall, cybercrime is "the transformation of criminal or harmful behaviour by networked technology,"[4] i.e., it developed as a result of the evolution of computerization and cyberspace and consequent new opportunities to attain, disrupt, or manipulate information for gain. Wall further classifies cybercrime into three categories: crime involving the integrity and good working order of computer systems (hacking); crime making use of cyberspace (encrypted communications among criminals, the sale of counterfeit pharmaceuticals); and crime involving computerized information contents (theft of secrets, dissemination of harmful contents).

Table 1 categorizes crime on the basis of the role played by the computer in the commission of the crime,[5] a position similar to that adopted by the European Convention on Cybercrime.[6]

Table 1. The Computer in Cybercrime

The computer as a tool in the commission of crime

Access to and dissemination of contents	Malicious disruption or modification of data	Use of communications
· Secrets · Knowledge/data · Harmful contents	· Identity theft · Fraud · Sabotage	· Harassment · Trade in forbidden materials · Spam

The computer as a target of crime

Unauthorized access	Inserting malicious code	Disruption of operation	Theft of service
· Hacking	· Malware, spyware, viruses	· Distributed denial of service (DDoS)	· Unauthorized use

There is nothing unique or new in much of cybercrime – harassment, fraud, unlawful propaganda, pornography, theft, money laundering, espionage, and so on – except the use of cyberspace. But there is another level of crime that could not exist without cyberspace: spam, click fraud, various types of malware, networks of captive computers (botnets),[7] digital identity theft, camouflage and encryption[8] of data and communications, computerized breaches of highly valuable secure facilities, and automatic, long term espionage in secure organizations, depriving them of control of intellectual property. Cyber criminals are exploiting the increasing value of digital data in all its forms, and the legal and judicial ways in which different countries handle cyberspace.

Crime has always been a widespread social phenomenon. Criminological explanations combine motivation, opportunity, and the existence of a "guarding" factor. Two different sources of human motivation can be identified.[9] Many motives for criminal behavior are intrinsic and are not determined through a cost benefit analysis. There is no reason to believe that greater use of one technology or another would change human behavior. It is therefore not surprising that people also use cyberspace to realize their needs and pursue their goals in legitimate activities – study, entertainment, education, work – as well as in the age-old human pursuits of warfare and crime.

The classic doctrine of criminology is based on the concept of free choice and a rational assessment of anticipated gain versus the risk of punishment; accordingly, the motivation for committing a crime is a rational economic decision.[10] Economists and psychologists analyze human behavior, including criminal behavior, as a derivative of a rational cost-benefit analysis. The ever-changing array of external circumstances may encourage cybercrime; this happens when someone identifies a growth in potential gain and estimates the cost – the risk of punishment – as being lower than that gain. The combination of greater digital connectivity in its current insecure form, and the increased value of computerized data results in a situation in which extrinsic motivation for criminal behavior rises.

Although developed nations have instituted regulated law enforcement mechanisms, state responses have not kept up with the pace of technological changes in cyberspace. A good example is the "traditional" bank heist as compared to cyber theft. In a traditional bank robbery security arrangements must be subdued as the chance of a confrontation with armed guards is likely. Even if the robbery itself is successful, the authorities will pursue the robbers for years to come. As cyberspace has developed, the exploitation of its vulnerability has also come to encompass bank robbery. For example, the use of botnets comprising tens of thousands of personal computers[11] for extended theft of identification details to banking sites, which are then used to steal small amounts of money, is quite common. Given the attribution problem in cyberspace, the chances of identifying the criminal are slim.[12] Financial institutions are well aware of the risk to their business interests and, together with regulatory bodies, are taking steps to protect themselves, investing in IT security to minimize the scope of opportunity available to cybercriminals. But even so, the immediate physical risk is still substantially lower for the cyber thief than it is for the "traditional" thief. The risk of legal punishment is lower as well, since cyber fraud is generally perceived by the judicial system as a non-violent "white collar" offense and treated accordingly.

The Scope of Cybercrime and Subsequent Damage: Problematic Assessments

The cybercrime phenomenon is usually examined from a variety of perspectives: legal (legislation and penalties), criminological (motivation and organization), economic (incentives and value), or technical (data

security). Jurists deal with setting the limits of what constitutes acceptable behavior and legal issues of prevention and enforcement. Criminologists apply their professional knowledge to understanding new phenomena. Economists describe the set of incentives affecting decision making by rational players. And data security experts deal with the technical aspects of technological infrastructures – software, hardware, and communications – while focusing on various vulnerabilities and ways to protect them. One thing that jurists, economists, and data security experts all agree on is that the scope and impact of cybercrime are constantly and rapidly on the rise. This assessment is based on the fact that the scope of digital data is increasing exponentially, as is connectivity between computerized facilities. Cyberspace contains more information with more potential access points for unauthorized breaches. The ordinary conclusion is that every breach exposes a growing scope of data.

Financial estimates of the scope of damage resulting from cybercrime have been issued since the 1990s, with security companies spearheading research into the subject and publishing numerous reports. There are dozens of different assessments emanating from the commercial and government sectors in the United States, England, and other developed nations.[13] An FBI report estimated damage to American business in 2005 at $65 billion.[14] In 2009, US Secretary of Commerce Gary Locke claimed that annual damage to American companies as a result of counterfeiting and piracy (i.e., illegal use of computer codes) was in the neighborhood of $200-250 billion.[15] A 2011 British report put damage at 27 billion pounds annually: the damage per annum to British citizens was estimated at 3.1 billion pounds, to the business sector at 21 billion pounds, and to the government at 2.2 billion pounds.[16] A recent report by Symantec, a leading global computer security software provider, estimated the direct damage caused by cybercrime at $114 billion annually in 24 nations.[17] Other estimates speak of hundreds of billions of dollars annually.[18]

These astronomical sums have raised question marks and doubts, but to date the impact of the criticism has been limited. Recently, two researchers at Microsoft published a position paper criticizing the shaky statistical infrastructure underlying assessments of cybercrime damage, which is typically estimated by surveys.[19] How have these estimates actually been carried out? An examination of research methods reveals how easy it is to produce inflated damage assessments. First of all, there is no information

about the use made (or not made) of data that was accessed. Those incidents where firm knowledge exists are few, whereas the scope of potential damage is huge. Let us assume that a PC storing a database of one thousand entries is breached; let us also assume that the database is not encrypted and the entries are written in plain text. Every entry represents a valid credit card, including all the information needed to use it: the number, CVC code,[20] expiry date, full name, ID number, and address of the cardholder, as well as the card issuer's bank information. In this scenario the thief sees a complete and real picture of the information on file. Yet even under these optimal circumstances, are we able to fully estimate the financial value of the information accessed? Can the thief properly assess the true value of the stolen information? Can the victim do so?

When it comes to the theft of intellectual property – the product of long research and development efforts – the victim tends to identify as damage the maximum profit he would have liked to make on completion of the R&D, manufacturing, and marketing process. Surveys, which are an appropriate method for clarifying hard-to-observe phenomena, are the main method of learning about the scope of damage. Surveys allow researchers to reach a larger, more diverse group of respondents providing their own estimates of the number of incidents and the damage, but they are also a method containing some serious drawbacks that concern social scientists and statisticians.[21] Secondly, in the absence of sufficient data, researchers use statistical methods to derive assessments from partial data.

Measurement problems affect every aspect of the debate on cyberspace threats, particularly attempts to help the discussion by quantifying damage in monetary terms. There is an inherent difficulty in estimating damage and so far it seems that monetary assessments – created by a crude use of statistical methods to present suppositions on the basis of insufficient data – are inclined to be inflated. In addition to questions of reliability of the research methods, the credibility of sources of information and the suitability of the statistical method to this type of research, there is also another problem. Monetary estimates often include indirect components of damage: whether to the reputation of the victimized organization, negative impact on consumer behavior with macro-economic implications, issues of torts, insurance, attendant expenses, or others.

Some questions central to understanding the phenomenon remain unanswered. Does it make sense to assess damage on the basis of use

actually made of the stolen information rather than maximum potential use? Perhaps it makes sense to relate to the monetary value of creating information instead of assessing its market value, present or future? And what about the cost of security and a return to normal functioning? The picture obtained from the usual sources is less than credible and the damage of inflated assessments is liable to result in a counter response of failing to take the power of cybercrime seriously enough. Basing the cybercrime debate on estimates of monetary damage detracts from a rational, intelligent, and informed debate on the problem and the ability to formulate appropriate public policy.

Cooperation between Criminals and Terrorist Organizations

The interface between professional criminals and organized crime on the one hand, and terrorist organizations on the other, is likewise not a new phenomenon. Even if we look only at the Israeli reality, we can see that such cooperation causes damage at the national level. Since 1996, the media campaign over pirated CDs has claimed that profits are used to fund Palestinian terrorism,[22] as part of a close connection between money laundering and its consumers such as terrorist organizations.[23] The widespread phenomenon of auto theft from Israel by West Bank thieves has been a feature of life in Israel for many years: the problem has hardly been confronted at national level because the threat was never considered to be a national security issue; the damage was covered by the insurance companies, which rolled it over onto the insured parties; the police took no action outside of sovereign Israeli territory; and the army – operating permanent security checkpoints on major roads – preferred to avoid dealing with a criminal population whose motivation was merely monetary, rather than nationalistic. During the "suicide bombers intifada" years the modus operandi of these criminals changed: terrorist organizations recruited the expertise of Palestinian car thieves in order to obtain cars with Israeli license plates to reach their destinations, and also to find routes to evade security checks and deliver explosives and suicide bombers into the heart of Israel's cities.

The possibilities of crossing over the fenced Gaza Strip border were more limited than between the West Bank and Israel. Tunnels were dug towards the Rafiah Egyptian border crossing to provide various kinds of smuggling channels. Smuggling generates large profits for the tunnels

operators and this activity persists despite Israel's efforts to put a stop to it. The tunnels also became a national security problem when they were used to smuggle weapons from the Sinai Peninsula to the Gaza Strip and terrorists from the Gaza Strip to Sinai.[24] It was the criminal organizations' expertise in digging tunnels that made the June 25, 2006 attack on Kerem Shalom possible, in which two soldiers were killed and a third was taken hostage by Hamas. This was a clear case of criminal technical know-how used to damage Israel's national security.

Some Bedouins in Sinai make a living from their expertise as guides and scouts, and have for decades provided smuggling services into Israel. The "goods" smuggled included, in the not too distant past, hundreds of East European women for the sex industry, as well as drugs. In recent years, tens of thousands of African migrant workers and some refugees have been guided to the Israeli border. Some believed these cases posed significant challenges but were not a national security issue. However, as the smugglers' expertise is increasingly applied to enable terrorist attacks on Israel, that assessment is changing.[25] The smuggling of terrorists from the Gaza Strip through Sinai to Israel made the August 18, 2011 attack on Route 12 possible, resulting in the killing of eight Israelis and the wounding of four. Smuggling terrorists and weapons has placed Eilat within rocket range.[26] Hence smuggling grew to become a clear and present danger to Israel's national security.

A Reexamination of the Meaning of Cybercrime

Any current examination of cybercrime reveals comparable commercial cooperation. In recent years a black market of technical experts and botnet "herders" has emerged, developing and providing technical tools and services for a price.[27] The black market of cyberspace services (Crimeware as a Service, or CaaS) causes economic damage in developed nations, though the usual monetary damage estimates are greatly exaggerated.

Anyone who prefers to operate alone and lacks R&D resources finds cyberspace weapons (toolkits of malicious software)[28] available for downloading from the internet, usually for payment of anywhere from tens to several thousands of dollars. Knowledge is an inexhaustible product, a "non-rival good" for economists, so sharing the capabilities that were available with others to you does not diminish your own strength.[29] As a result, we see a situation in which powerful tools are available to anyone

at marginal cost. The widespread impression that cyberspace makes it easier to rake in huge profits from criminal enterprises has not been lost on organized crime.[30]

Growth in computing power and the ubiquitous internet have created a new tool for extensive cybercrime: the botnet. This is a collection of internet-connected PCs whose defenses have been breached by malware and control ceded to a malicious third party, who is able to remotely control and exploit these computers on demand, usually without disrupting their normal functioning. Cybercriminals usually infect internet-connected computers with malware by exploiting known vulnerabilities that users and system administrators have failed to deal with. In 2007, McAfee estimated that some 5 percent of all internet-connected personal computers were botnet captives.[31] Large scale supply makes the cost of using a botnet affordable to virtually anyone.[32]

A newer phenomenon is the advanced persistent threat (APT), also known as adaptive persistent attack (APA)[33] – a complex, multi-stage use of cyberspace weapons for the purpose of ongoing clandestine attacks. The attacker does not operate statistically on a broad scale to exploit known vulnerabilities; instead the objective is well defined. The attacker uses a range of custom made tools, often using a valuable "zero-day" (never used before) attack mechanism. Such attacks comprise several stages and can last months or even years. The attacker begins to gather intelligence about the organizational structure of the target, and identifies people holding senior positions with access permissions for sensitive information. The gathering of personal information is usually accomplished by open source intelligence (OSInt): accessing public information and shared personal information on social networks and the news media. Once the key players are identified, a concerted effort is undertaken to steal their credentials and infect their computers.

One method is spear phishing, or inserting a remote access tool (RAT) by an email from a trusted sender with relevant content, which thus manages to bypass spam filtering mechanisms by using the personal information gathered. Opening the email allows the insertion of the Trojan horse into a trusted endpoint inside the organization's corporate network, thus gaining access to more internal resources. In a common crime, once access is accomplished, the average attacker moves quickly to retrieve valuable information and use it.

However, this is not the case with an APA attack: here the purpose is clandestine long term access, ignoring immediate monetary temptations. The attack lasts a long time, in part to overcome defense systems designed to prevent information leaks. In the course of the attack, attackers perform tests to identify the system's response thresholds and usually adapt the exfiltration methods of the stolen information. The data is divided into small packages, camouflaged inside legitimate communications, and thus leaks through the system without triggering defenses. An APA is much rarer than statistical attacks because it is much more expensive, requiring systematic intelligence gathering, planning, and adapting capabilities and the patience to carry out a long term task. Correspondingly, the damage of an APA is of a different scale.[34]

From the economic perspective, in terms of supply, hacker groups that have succeeded in developing and using software tools to control tens of thousands of computers have in fact created a service of economic value. In terms of demand, various customers − other hackers, private investigators, criminals, espionage organizations, and transnational criminal organizations − have found various uses for the product. This has created the "Crimeware as a Service" (CaaS) model, the black market counterpart to "Software as a Service" (SaaS) which has served the IT industry since 2001.[35] Over the years the model has undergone several transformations; the current buzzword for it is "cloud computing." The economic justification of the model is clear: from now on, the customer no longer needs to buy computer equipment in order to use computer services; he can simply buy the specific service he needs from large operators and use it over standard communications. The scope of the global market for this type of computer service was estimated at $14.5 billion in 2012.[36]

Let us examine the black market phenomenon from the national security perspective. The existence of a black market of cyber weapons, outsourcing research and development, quality assurance services, and technical support means that the requisite level of technical skills to become a cyber criminal has dropped. No longer is it necessary to have the competence to develop tools and methods for breaching computers oneself. The technological infrastructure needed to breach and make unauthorized use of computers is the same, regardless of whether the breach is aimed at profit, sabotage, terrorism, or destruction.[37] This reveals another risk: the use of existing tools for terrorist activity and damaging

critical infrastructures – rather than the expected fraud targets for theft and quick profits – threatens to damage national security. The continuing development of cybercrime mechanisms is therefore becoming a natural security problem.

Critical infrastructures protection (CIP) is the most important issue in cyberspace security, and the black market in cyber weapons makes the need for it even more acute. This commercialization of technical and operational capabilities allows access for many factors – including small terrorist organizations and even isolated individuals – to powerful resources with potential cyber attack application. The reference group of threats is therefore expanding beyond states and known terrorist organizations to include any element capable of purchasing commercial services available on *DarkMarket*. Nonetheless, when there is ongoing state-sponsored investment in R&D, the technological capabilities openly available on the market naturally lag behind those being developed by the security forces and a nation's institutions of higher education. Therefore the capabilities available on the market will be inferior to those accessible to state-sponsored organizations with independent R&D means, enjoying state backing in terms of resources and organization.

Towards Realizing the State's Responsibility for Cyber Security

The meaning of the cybercrime phenomenon needs to be clarified for researchers and policymakers. For the reasons stated above, monetary damage assessments do not provide a firm factual basis for understanding the concept or formulating policy. Therefore, a reassessment of cybercrime is required to design appropriate national policy.

Even in the absence of agreement on the scope of direct and indirect damage caused by cybercrime, it certainly affects how citizens, organizations, and society as a whole function. Citizens and small businesses are variously damaged by cybercrime. Spam, internet fraud, digital identity theft, invasion of privacy, blackmail, economic espionage, and damage to intellectual property all are widespread and harm some citizens and organizations. Although monetary assessments seem to be exaggerated, the development of cyberspace increases numbers of potential victims and expands even further ways of committing crimes against citizens and groups. Given rising awareness of the problem and the actual increase in cybercrime, citizens of developed countries will

reasonably demand the state take steps to provide personal, communal, and national cyber security. Growing media exposure of data breaches and cyber attacks is indicative of a proportionate growth of interest in the risks posed by cybercrime.

The state is fundamentally responsible for law and order and for the safety of its citizens, and is required to act to minimize damage to them. Policy should develop on the basis of understanding the broad implications of the phenomenon and a rational, informed public debate. Below are some pointers for developing such a debate.

The majority of the common phenomena classified as cybercrime have nothing to do with national security. What, then, is the significance of spreading hatred and incitement against Jews or the State of Israel while defacing Israeli websites, disseminating propaganda by means of social media and spam, hijacking social networks accounts, and creating internet videos and campaigns offensive to the public? Citizens will be vulnerable in cyberspace and the dignity of the nation and many of its citizens will be subjected to slander and defamation. However, experience shows that the public is not easily shaken by such acts. Beyond the professional realm of public relations, the damage at the national level is negligible.

What is the significance of common fraud – digital identity theft and unauthorized use of means of payment information aimed at stealing from citizens? When a citizen becomes a crime victim, the state authorities are expected and required to address the crime and deal with it. The state authorities have a range of methods to this end and the meaning of the events needs to be clarified so as to determine the appropriate policy. But from the perspective of national security, it is hard to see damage at national level as long as the rate of cybercrime is relatively low, even if it is higher than the more conventional crime rate. If, however, cybercrime grows to become a lasting and widespread phenomenon, citizens might lose their faith in state authorities that seem unequal to providing a safe and secure environment.

The current situation in developed nations is far from satisfactory. If "obedience in exchange for protection" is the condensed version of the social contract between citizens and the sovereign, then in the cybercrime area the state is defaulting on its side of the contract. Response to the new challenges requires, first and foremost, a clear understanding of the different phenomena and their implications and ramifications. Response

processes and the formulation and enforcement of policy require updated regulation and legislation. Legislation, which by definition lags behind technological developments, lies within the sole purview of the state. The sovereign enforcement bodies operating on the basis of national legal infrastructures will have to allocate more resources to the prevention, investigation, and punishment of cybercrime. Despite the international nature of cyberspace, the state is the sole source of responsibility for the personal security of its citizens. International treaties such as the European Council's Budapest Convention on Cybercrime[38] and initiatives being developed in the UN,[39] the OECD,[40] the EU,[41] and the International Telecom Union[42] are all boosting cooperation among sovereign authorities. International cooperation may contribute to arming sovereign authorities in the fight against cybercrime, but international treaties cannot substitute for independent sovereign policy.

First, cooperation among nations in the anarchic international arena is possible only to a very limited extent and only on the basis of common interests. It may be that developed democracies will be able to formulate arrangements among themselves, but the gap between them and authoritarian regimes in terms of defining the threat seems too great. The American debate on the issue focuses on ongoing industrial espionage of intellectual property, the product of R&D in the commercial and government sectors in the United States. Over the years, senior personnel in the business and government community have become increasingly concerned about the loss of America's global economic and strategic advantage as the leading scientific-technological innovator and superpower. In fact, "loss" is not the right word, because the knowledge is not actually lost, but rather stolen through systematic, well-organized and widespread state-sponsored theft, and the culprit is China, a nation determined to catapult its economic and military might forward by copying the secrets of American research.[43] Hence discussion of the issue clearly shifts from focusing on the economy, data security, and the law, to an almost combative security dialogue.[44] For its part, China rejects these allegations outright and is worried about undermining the foundations of its regime by use of the West's internet in the name of freedom of expression.

Second, the authority and sovereignty of a state within its borders allows that state to promote independent policy: legislation and law enforcement are not dependent on international arrangements. In Israel, an

incident known as the "Saudi hacker affair" demonstrates how the debate spills over from data security into national security. In early January 2012, someone calling himself OxOmar published a list containing the personal information and credit card numbers of thousands of Israeli citizens.[45] The information published was overwhelmingly outdated, and out of 380,000 entries only a few thousand were valid. The direct damage to cardholders was zero: the credit companies cancelled the cards and issued new ones, and in any case the law obliges them to cover unauthorized use. The scope of the information revealed was also not exceptional: every day, millions of such entries are stolen on the internet. The details are bundled according to different parameters and sold as dumps[46] to black market customers, as described above.

It soon became clear this was a simple attack: spyware had been inserted into a number of commercial Israeli websites, which transferred data stored by the site operators with gross disregard for data security. Although the attack lacked complexity and no real damage was incurred by the Israeli citizenry, the extensive media coverage of it lasted some three weeks and was initially tinged with panic and hysteria. The event was presented as anti-Israeli terrorism, because instead of realizing monetary profits from the information, the attacker chose to use it to propagate fear in the target country.

This event can be analyzed in any number of different ways. One may claim that citizens are unaware of data security; that the media are irresponsible and blow a marginal event out of all proportion, sowing panic; that website owners were careless or even criminally negligent in failing to secure the data in their possession; that the state neglected to create a safe environment for internet commerce and secure personal data. But in any analysis, the inevitable conclusion is that the personal and collective security of Israel's citizens in cyberspace needs to be upgraded. At the end of the day, that demand is directed at the state, which is responsible for its citizens' security and safety.

It is possible, even desirable, to discuss the definition of unwanted and criminal phenomena in cyberspace, the proper level of security, the division of responsibility, heightened user awareness, the limits of state involvement, and other dilemmas relevant to the matter. In a democracy, such issues are clarified through public discourse and political process. It cannot be assumed that the demand for cyberspace security will disappear,

that the problem will go away, or that the state will be able to shrug off its responsibility towards citizens. In the aforementioned Israeli case, nothing exempts the state authorities from responding to various citizen demands and undertaking legal and regulatory changes to increase data security on commercial websites. Failure to regulate and enforce law and order in cyberspace will enable a range of cybercrime to flourish, to the point of real threats to national security: providing service to hostile elements aiming to carry out cyber attacks and increasing the scope of crime to the point of compromising both personal security and the nation's business environment.

A Dangerous Interface: Cybercrime as a National Security Threat

Cybercrime continues to grow and challenges developed nations in different ways. Existing information about cybercrime is acquired from periodic reports by consulting, IT and information security companies, and law enforcement agencies. Given the problems inherent in identifying the phenomenon, the crude use of statistical methods for a quantitative analysis, and the inclusion of indirect damage in monetary assessments, it is apparent that existing information is not reliable. It seems that monetary assessments are consistently inflated. Nonetheless, that there is great potential danger in cybercrime cannot be overlooked.

The analysis in this article shows that in effect a large range of cybercrime does not represent a threat to national security. Phenomena such as theft and industrial espionage, fraud, harmful contents, hate crime, destruction of websites, denial of service, and so on are liable to become a national security problem only if there is a marked increase in their incidence and their effects are lasting. Therefore, now is the time to take action to reduce the risk and make it more difficult for cybercriminals to operate in this realm.

Past experience shows that hostile elements recruit criminal expertise to achieve operational goals. Because of the pace of technological developments, what today are advanced IT capabilities will within very few years become inexpensive, off-the-shelf commodities. The black market of computer services makes advanced capabilities readily accessible. The evidence exacerbates the concern that in cyberspace too, cooperation among criminal elements and hostile entities exists and is on the increase.

On the basis of this analysis, focus on two major interfaces between cybercrime and national security is recommended. First, the nation state is the entity responsible for the personal and collective safety and security of its citizens. Cybercrime causes various kinds of damage to citizens and organizations. The scope of such damage is unclear and the various damage estimates proffered in the debate are largely unreliable and exaggerated. But even without agreement on the scope and damage incurred by citizens, organizations, and states, the state must still respond to the opportunities and challenges of the reality as it unfolds. With the ongoing entry of cyberspace into every walk of life, it is safe to assume that demands on the state to assure personal and national security in cyberspace will also grow. Despite the global nature of cyberspace, the state will be forced to expand its involvement considerably. The outline of state involvement in cyberspace has been emerging in recent years, one of the more loaded issues being the mutually contradictory values of privacy and national security. In a democracy, the process for formulating a government policy on cybercrime involves public debate, political battles, and long term legal treatment.

Second, the commercialization of technical and operational capabilities is lowering the threshold for entering the cyber warfare arena, expanding the reference threats beyond states and large terrorist organizations, and placing a very heavy burden on national security authorities. Cyber criminal organizations offer resources, infrastructures, and even customer service at reasonable cost. This is a market that can be exploited not only to commit crime for financial profit but also to carry out direct attacks on national security. Defending critical infrastructures against cyberspace threats is a key issue in cyber security and its importance is even greater given the prevalence of potential elements of risk capable of acquiring cyberspace weapons and recruiting "fighters" on the cyber criminal black market.

Given the analysis of the phenomenon's significance and the identification of dangerous interfaces between cybercrime and national security presented herein, the immediate state focus should be on dealing with the threat in order to prevent it becoming more acute. The state must upgrade its involvement in creating cyberspace security, but it cannot solve the problem alone. The successful realization of state responsibility for cyberspace security necessitates the cooperation of all interested parties

in the business, academic, public, and security sectors, so as to provide national and personal cyberspace security to the state and its citizens.

Notes

1 P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies,* 10, no. 2 (2001): 243-49.

2 Majid Yar, *Cybercrime and Society: Crime and Punishment in the Information Age* (London: SAGE Publications, 2006).

3 D. L. Shinder and M. Cross, *Scene of the Cybercrime* (Burlington, MA: Syngress, 2008).

4 David S. Wall, *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge: Polity, 2007), p. 10.

5 A. Alkaabi, G. M. Mohay, A. J. McCullagh, and A. N. Chantler, "Dealing with the Problem of Cybercrime," Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, October 4–6, 2010, Abu Dhabi, http://eprints.qut.edu.au/38894/1/c38894.pdf.

6 CoE, "Convention on Cybercrime," Budapest, 2001, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

7 A botnet is a collection of internet-connected computers whose defenses have been breached and control ceded to a malicious party gaining distance control and using these computers' capabilities. A botnet is commonly used for sending spam, attacking DDoS, and continuous data theft. See https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html.

8 Asymmetric key cryptography is the basis of the RSA algorithm developed by Leonard Adelman, Adi Shamir, and Ron Rivest, and presented publicly in 1978. Its patent expired in 2000. PGP (Pretty Good Privacy) developed by Phil Zimmermann in 1991 was the first software to allow free use of strong encryption using this method . The common web security standards (HTTPS, TLS/SSL, SSH, Bitcoin) are employing the same public key cryptography principle.

9 Richard M. Ryan and Edward L. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology* 25, no. 1 (2000): 54-67.

10 A. R. Piquero and Stephen G. Tibbetts, eds., *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (New York: Routledge, 2002).

11 The number of infected computers is itself no indication of the network's power or potential damages. See Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, *Botnets: 10 Tough Questions* (ENISA, 2011).

12 Wall, *Cybercrime,* p. 221.

13 See for example the GAO-07-705-Cybercrime Report, June 17, 2007, pp. 16-17, http://www.gao.gov/assets/270/262608.pdf.

14 "2005 FBI Computer Crime Survey," p.10, www.fbi.gov/publications/ccs2005.pdf.

15 Melissa E. Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," ch. 6, in *Securing Cyberspace: A New Domain for National Security* (Queenstown: Aspen Institute, February 2012).

16 Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica,: "The Cost of Cyber Crime," 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

17 "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually," http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

18 M. Lesk, "Cybersecurity and Economics," *IEEE Security & Privacy,* 9, no. 6 (2011), p. 76; Carl Bialik, "A Cybercrime Stat's Nine Lives," *Wall Street Journal,* September 26, 2007, http://blogs.wsj.com/numbersguy/a-cybercrime-stats-nine-lives-194/tab/print/.

19 Dinei Florêncio and Cormac Herley, "Sex, Lies and Cybercrime Surveys," Microsoft Research, 2012. The study was condensed and appeared as an op-ed piece in Dinei Florêncio and Cormac Herley, "The Cybercrime Wave That Wasn't," *New York Times*, April 15, 2012, https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=3&hpw.

20 Card Verification Code – the secret three-digit code printed on the back of credit cards, used to verify the validity of the card details when the card is not being read magnetically.

21 This discussion exceeds the scope of the present article. For a good overview, see the chapter on surveys in Francis C. Dane, *Evaluating Research: Methodology for People Who Need to Read Research* (Los Angeles: Sage, 2011).

22 "Counterfeit CDs are Money for Islamic Terrorism," *Ynet*, January 16, 2003, http://www.ynet.co.il/articles/0,7340,L-2378873,00.html.

23 J. Hunt, "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them," *Information and Communications Technology Law* 20, no. 2 (2011): 133-52.

24 Israel Security Agency, "Report on Hamas' Use of Underground Passages in the Gaza Strip," November 2008, http://www.shabak.gov.il/publications/study/Pages/hamas-tunnel-report.aspx.

25 Israel Security Agency, "Smuggling Weapons to the Gaza Strip from Iran via Sudan and Sinai," http://www.shabak.gov.il/publications/study/Pages/Sudan120511.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93 .

26 Meir Amit Intelligence and Terrorism Center, http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/ipc_272.htm.

27 Nir Kshetri, "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures," in Nir Kshetri, ed, *The*

Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives (Heidelberg; London: Springer, 2010); Misha Glenny, *Darkmarket: Cyberthieves, Cybercops, and You* (New York: Alfred A. Knopf, 2011).

28 Cyber weapons may be categorized by their intended usage: malware − malicious software meant to disrupt the normal workings of a computerized system clandestinely, thereby damaging the process controlled by that system; spyware − malicious software meant to gather data clandestinely and sometimes transfer it over the internet; scanners to identify known vulnerabilities; remote and local exploits − to exploit known vulnerabilities; network sniffers − to eavesdrop on communications; backdoor tools, Trojan horses − for distance access and data retrieval.

29 See Isaac Ben-Israel and Lior Tabansky, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 3 (2011), p. 24, http://www.inss.org.il/upload/(FILE)1333532835.pdf.

30 Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues* 6, no. 2 (2001): 5.

31 McAfee, "Virtual Criminology Report: Organized Crime and the Internet," December 2007, www.mcafee.com/us/research/criminology_report; C. Czosseck, G. Klein, and F. Leder, "On the Arms Race around Botnets: Setting up and Taking Down Botnets," paper presented at the Cyber Conflict (ICCC), 2011 3rd International Conference, June 7-10, 2011.

32 "Kaspersky Reveals Price List for Botnet Attacks," July 23, 2009, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnet-attacks. It seems that the cost continues to drop. See Plohmann, Gerhards-Padilla, and Leder, *Botnets: 10 Tough Questions.*

33 Jeffrey Carr, November 2, 2011, http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html.

34 All high profile cases of cyber espionage, such as "Gh0st RAT," RSA/Lockheed-Martin, and "Flame" are examples of an APA.

35 *Software as a Service: Strategic Backgrounder* (Washington, D.C.: Software & Information Industry Association, February 28, 2001), http://www.siia.net/estore/pubs/SSB-01.pdf.

36 https://www.gartner.com/it/page.jsp?id=1963815.

37 Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92, http://www.inss.org.il/upload/(FILE)1308129610.pdf.

38 CoE, "Convention on Cybercrime." Since 2001, the convention has been ratified by 30 of the 46 signatory nations.

39 T. Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities regarding Cybersecurity," Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

40 OECD, "Communiqué on Principles for Internet Policy-Making," June 29, 2011.

41 EU, Europol, the European Cybercrime Centre (EC3) officially commenced its activities on January 1, 2013, https://www.europol.europa.eu/ec3.

42 ITU, *National Cybersecurity Strategy Guide*, September 2011.

43 Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is National Policy-and Must Be Challenged," *Wall Street Journal*, January 27, 2012; Richard Clarke, "How China Steals our Secrets," *New York Times,* April 2, 2012; Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly* 27, no. 2 (2010):15-17; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011); U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission.*

44 See Myriam Anna Dunn and Kristian Søby Kristensen, eds., *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security* (London: Routledqe, 2007).

45 Ro'ee Goldenberg, "The Bank of Israel: Details of 15,000 Credit Cards Stolen," *Globes*, January 3, 2011, http://www.globes.co.il/serve/globes/printwindow.asp?did=1000712125; Yazan al-Saadi, "Saudi 0xOmar: Hackers of the World Unite Against Israel," *al-Akhbar English,* January 16, 2012, http://english.al-akhbar.com/node/3413.

46 Dump: a stolen credit card or bank account and the associated customer data. T. J. Holt, and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies* 23, no. 1 (2010).

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for publication in *Military and Strategic Affairs*, a refereed journal published three times a year in English and Hebrew and edited by Gabi Siboni, Director of the Military and Strategic Affairs Program and Cyber Warfare Program at INSS.

Articles may relate to the following issues:

- Military and strategic thinking
- Lessons learned from military organizations throughout the world
- Military force developments on various subjects, including: human resources, weapon systems, doctrine, training, command, and organization
- Ethical and legal aspects of war and combat
- Military force deployment and operations
- Civil-military relations and decision making processes
- Security/military technology
- Cyber warfare and critical infrastructure protection
- Defense budgets
- Intelligence

Submitted articles should not exceed 5500 words (including citations in standard format) and should be accompanied by an abstract of 200 words. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

Submissions should be sent to:
Daniel Cohen
Coordinator, *Military & Strategic Affairs*
danielc@inss.org.il