Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 3 | Issue 1 Article 3

2018

Sticking to their Guns: The Missing RMA for Cybersecurity

Lior Tabansky
Cyber Security Group, cyber.ac.il@gmail.com

Sticking to their Guns: The Missing RMA for Cybersecurity

Cover Page Footnote
This research was partially supported by a grant from the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University (TAU). The paper presents the author's personal opinion.

Sticking to their Guns: The Missing RMA for Cybersecurity[1]

Lior Tabansky[2]

Abstract: Why has cybered conflict disrupted the security of the most developed nations? A foreign adversary contemplating an attack on a developed nation's heartland certainly faces multiple state-run military-grade lines of defense on land, sea and air. A foreign adversary launching a direct cyber-attack on a non-military homeland target will meet none. Armed forces do not shield a society from cyber-attacks originated by foreign adversaries, no longer provide a buffer between the enemy and homeland, nor can they identify the attacker after an attack occurred.

Adversaries succeed in waging cybered conflict against the U.S. and its allies. Having repeatedly inflicted economic and social harm while evading retaliation, adversaries become brazen. To prevail in cybered conflict, we need to return to the very foundations of our defense.

However, profound defense adaptation is especially problematic for dominant militaries. To develop my argument, I turn to analyze a Stuxnet-like scenario using the Revolution in Military Affairs (RMA) concept of Security Studies and the paradigm shift concept of philosophy of science. Security Studies theory, philosophy of science and empirical evidence all suggest that profound defense adaptation demands pressure from outside the expert organization. I argue that Security Studies theory and empirical evidence, including Israel's defense adaptation following short-range rocket threat, suggest that civilian outsiders coalescing with military partners can successfully drive defense adaptation.

To secure the Western world order, the U.S. and its allies need to rearrange their security forces, leveraging the experience accumulated through centuries.

[1] Please cite as: Tabansky, Lior, "Sticking to their Guns: The Missing RMA for Cybersecurity," in Demchak, Chris and Benjamin Schechter, eds. *Military Cyber Affairs: Cyber, Economics, and National Security* 3, no. 1 (2018).

[2] Scholar of cyber power at Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center (TAU ICRC)

Cyberwarfare is Raging in the Homeland

Chinese bulk espionage and its heavy economic toll has long been the main cybered threat to the U.S. (Brenner & Lindsay, 2015; Cheung, 2009; McConnell, Chertoff, & Lynn, 2012). In 2010, a direct destructive cyber-attack on computerized Industrial Control Systems (ICS) at a hardened homeland target became a reality (Demchak & Dombrowski, 2011; Denning, 2012; Zetter, 2014). Ransomware has crippled numerous devices and networks in small business and homes ("Verizon report shows business is booming for cyber-criminals," 2017). Foreign state-sponsored adversaries have successfully carried out politically-motivated attacks against civilian targets in the U.S., including Sony Pictures Entertainment (Sharp, 2017) and Sands Casinos (The Australian Strategic Policy, 2015). Hostile cybered influence operations targeting the democratic process have recently emerged on the cybered conflict agenda (Kragh & Åsberg, 2017; Kramer & Wentz, 2008; Tabansky, 2017). Cyberwarfare is raging at homeland: cyber-attacks have hit power production, financial services, numerous industries and political processes.

Despite decades of threat awareness, leading technology, superior budgets and capability development, the residual cyber risk to developed nations has skyrocketed. The U.S. Director of National Intelligence has ranked cyber as the top national security risk since 2014, taking over the top spot held by terrorism post- 9/11. Why have cybered threats disrupted the security of the most developed nations? I argue that armed forces have failed to adapt strategically to cybered conflict. Ministries of defense and militaries are bystanders in raging cyberwarfare. This profound national cyber insecurity in the leading states demands scrutiny.

First, I develop the analysis with the fundamental strategic theory guiding every sovereign defense. Using a Stuxnet-like scenario I show how cybered conflict challenges the very fundamentals that we grew accustomed to and treat as axioms. Having established the need for profound defense adaptation, I review the studies of maladaptation – two in the United State and one in Israel -- to stress that obstacles to defense adaptation are conceptual rather than technical. I conclude with a discussion of how to facilitate profound change by presenting and analyzing one recent successful innovation in Israel's defense.

DOI: https://doi.org/10.5038/2378-0789.3.1.1039

Where We Are: Armed forces vs Stuxnet-like attacks in the US and Israel

To put a comfortable excuse to rest, cybersecurity is not new to the Western defense community. The quarter-century-old U.S. National Research Council report reads as if it were written today:

> *We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable – to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack* ((U.S.)., Board., & System Security Study Committee., 1991).

Presidential Decision Directive No. 63 (PDD-63) of 1998 set the ability to protect the nation's cyber-physical systems (CPS) in critical infrastructure from intentional attacks (both physical and cyber) by the year 2003 as a national goal. The scenario has become real:

The 2015 U.S. National Security Strategy reiterated the fact that foreign states attack the U.S. homeland targets in cyber:

> *Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure United and President,* "National Security Strategy," (Washington, DC: The White House, 2015). pp. 12-13, Emphasis added.

However, the U.S. federal response outside of the Department of Defense (DOD) remains light, indirect and self-constrained to voluntary action. U.S. military forces now prepare to fight in five domains: land, sea, air, space and cyber. To address the national security implications of cyberspace, the DOD has identified cyberspace in military strategy and doctrine as an operational domain in which to organize, train and equip forces to ensure it has the necessary capabilities to operate effectively across all operational domains of warfare.

Notably however, the DoD plays a supporting role to the DHS. The DoD only steps into Critical Infrastructure Protection action *after* a severe incident has occurred, caused damage and

has been identified. Defense Support of Civil Authorities (DSCA) is the process by which the DOD may provide support through the federal military force, National Guard, and other resources *in response to requests for assistance from civil authorities for domestic emergencies* (e.g., hurricanes and wildfires), special events (e.g., political party national conventions), designated law-enforcement support and other domestic activities. The National Response Framework (NRF) outlines a tiered process in which incidents are generally handled at the lowest jurisdictional level, providing a process for a state governor to request assistance from the President prior to DoD involvement. Only if directed by the President or SecDef (likely following a state-level request), the DoD may be required to bring its immense capabilities to conduct Cyber-DSCA.

In Israel, the recognition of cyber risks and threats to civilian cyber-physical systems came later than in the U.S. With an understanding of civilian infrastructure and cyber-vulnerabilities garnered from decades of defense experience, in the late 1990's defense leaders communicated cybersecurity concerns to the civilian government. These concerns are today referred to as risks to CPS. Quoting the key person involved:

> *In the mid-1990s we in the defense community were looking for suitable targets for cyber exploitation around us [Israel]. Quickly we realized that by far the largest set of targets exists – but it is Israel.*[3]

The head of MAF'AT (the Ministry of Defense Directorate for Defense Research & Development, DDR&D) at that time personally took the initiative to address the government on several occasions, raising the issue of new society-wide vulnerabilities for the first time. However, the Israeli policy response differed markedly from the U.S., as the state accepted much higher role in defending the civilian sector. By the end of 2002, the efforts to develop a national Critical Infrastructure Protection (CIP) arrangement culminated in Government of Israel Special Resolution B/84 on 'the responsibility for protecting computerized systems in the State of Israel.' Notable in the 2002 resolution is that what today is referred to as 'cyberspace' was not viewed as a virtual environment, or as an independent area of operation. The subject of protection - 'computerized information systems' - were defined as being interconnected with physical realms. Moreover, an 'information' system differentiates from a 'control' system in both concept and practice. An information system 'performs automated activities of input reception, processing,

[3] Personal interview with B., Tel Aviv 2014

storage, processing and transmission of information.' A control and supervision system, on the other hand, is 'a computer-integrated system that controls and supervises the frequency and regulation of measurable activities, carried out by mechanized means within the information system itself.'[4]

The defense sector - especially some specific IDF units - had leading IT-security expertise. But Israel also rejected a military-centered cyber CIP approach. Designating responsibility for protection of vital computerized systems of civilian bodies to the military in peacetime would create an immense ethical and legal problem for the Israeli democracy. Moreover, given the technical characteristics, delineation of domestic versus foreign ceased to be clear.

In the U.S. and in Israel, the cybered threats to the homeland continued to grow and materialize in various ways. In response, the ministries of defense and armed forces led the development of human capital, technology and doctrine, even running offensive operations in cyberspace. However, none of the ministries of defense and armed forces have been tasked with the leading CIP role, nor a bigger role in protecting the respective societies. The U.S. upholds the voluntary approach to Critical Infrastructure Protection, and the DoD's vast resources can only be utilized after disaster strikes. Despite Israel's state-led defense of Critical Infrastructure and cyberspace in general, Israel does not utilize the MoD's or IDF's expertise and vast resources for these tasks.

The common cyber defense position is that armed forces cannot be responsible for defending society from cyber-attacks on strategic non-military homeland targets by foreign adversaries. National cybersecurity tasks and associated practices require a presence in domestic networks, while existing laws prohibit the armed forces from domestic operations. Armed forces have been adapting to cybered conflict: navies seek to leverage new technologies to improve the effectiveness in the seas; air forces do the same in the air, and so forth. The doctrine remains largely intact, with cyber technology playing only a supporting role to existing concepts of operations. This kind of adaptation is not only rational but also required by the applicable laws.

[4] (Tabansky, 2013)

I argue that the defense adaptation that has been progressing is in fact misguided. I do not refer to the pace of change, nor to resource allocation. The main problem is the misguided direction of change, as it has neglected the drastic transformations brought on by cybered conflict.

To understand the challenges of cybered conflict, we need to drill down deeper than usual with regard to defense adaptation. To develop my argument, I turn to analyze a Stuxnet-like scenario using the Revolution in Military Affairs (RMA) concept of Security Studies and the paradigm shift concept of philosophy of science.

Winning the next war? The Fundamental Strategic Theory Challenge

The guiding strategic assumptions of national defense have been formed as a result of decades and centuries of experience in war. In every modern state armed forces play the central role in defending the nation against foreign adversaries. As Demchak and Dombrowski wrote in 2011:

> *Most nations make a distinction between the forces defending the borders from attack (militaries) and those protecting the individual citizens inside the nation from attack (police). This distinction is one of the direct outcomes of the rise of the modern state from the Westphalian Peace. But it is severely challenged by the unfettered character of the current global cyberspace topology. Today militaries, police, and intelligence organizations in particular have been challenged both by the attacks and by the jurisdictional lack of clarity in obligations and ability to demand resources. Both state and nonstate competitors have used the interconnectivity inherent to the web to attack and disrupt operations and gather intelligence about capabilities and intentions across borders with impunity.* (Demchak & Dombrowski, 2011) p. 43

Across the strategic security studies literature and lessons from history, one can argue that a 'fundamental strategic theory'[5] lies behind every sovereign defense strategy and relies directly on the armed forces performing both defense and deterrence missions in protecting the state. The following set of axioms and corollaries summaries and capture what are the key elements of these two missions. Armed forces are expected to:

1. Defend and fight when hostilities have erupted: armed forces defend the nation's society, economy and citizenry from harm:

[5] This summary is the author's own.

   a. Prevent the enemy force (soldiers and weaponry) from reaching the nation's homeland as demarcated by borders.
   b. Sustain the bulk of damage, while the citizens are safer at homeland. Military units maneuver and fight on a battlefield, preferably not within own borders.
   c. Buffer between the enemy and society: borders, barriers, forward deployment, conquest of enemy territory to push back farther than the effective range (e.g. Israel-Lebanon 1982 war, 40km range)

2. Deter hostilities: armed forces deter the enemy so that hostilities do not erupt at all or do not escalate:
   a. Assess adversarial intent and capabilities through intelligence services and in collaboration with other defense agencies.
   b. Identify swiftly and reliably the attacker(s) responsible for the attack.
   c. Engage in battle to punish the attacker(s) responsible for the attack to demonstrate will and capability in order to deter further attacks and other would-be attackers.

While the list above should appear straightforward to the reader, cybersecurity poses particularly difficult challenges for defense and deterrence in national security. The U.S. armed forces and the Israel Defense Force (IDF) are well aware of the fact that each war will play out differently from the last one. Efforts to think about how the next conflict will play out and what needs to be done to prevail are evident across both forces, but so far these efforts have fallen short of what is needed.

The Missing Cyber RMA in the West

Security Studies scholars have long researched changes in militaries and the historical conditions of victory and defeat. The Security Studies "Revolution in Military Affairs" (RMA) concept developed separately from the original Kuhn definition of a changing paradigm[6], but the

[6] The Security Studies scholarship on military innovation and Kuhn's seminal study of scientific communities independently reach very similar findings: the obstacles to defense adaptation are conceptual and organizational rather than technical. I turn to focus on just one aspect: the significance of professional expertise.
In science, a paradigm refers to universally recognized scientific achievements that, for a time, provide model problems and solutions for a community of practitioners. A paradigm represents a set of "concrete puzzle solutions" which the associated community employs as "models or examples" to "replace explicit rules as a basis for solutions of the remaining puzzles of normal science."

RMAis defined as *a paradigm shift in military operations that obsolesces one or more core competencies of a dominant player or creates one or more new core competencies.* (Hundley, 1999) Many historical RMAs came as the result of a military organization applying new technologies coupled with innovative operational concepts to gain new competencies. With these new competencies, armed forces achieved operational goals in a new manner that rendered their opponents' defenses obsolete. Historical evidence shows how a normal period of defense may be periodically punctured by revolutionary outcomes such as one-sided victories achieved when one force renders opponents' defenses obsolete. These RMAs usually occur after building upon long periods of peacetime defense adaptation.

Today this adaptation process can be studied in near real-time. A successful and direct destructive cyber-attack on civilian critical infrastructure, for example, meets the definition of an RMA. In this case, it is the success in the application of new technologies - with innovative operational concepts and organizational adaptation to gain new competencies that demonstrates the RMA capable of achieving operational goals in a new manner that renders existing defense systems obsolete such an attack is a genuine threat, as proven with the discovery of Stuxnet in 2010.

Kuhn introduced the concept "paradigm shift" to describe a fundamental change in the basic concepts and experimental practices of a scientific discipline. Kuhn contrasted these shifts to normal science, which he described as scientific work done within a prevailing framework (or paradigm). Similarly, normal defense works well when the basics of the discipline remain unchallenged by a growing number of anomalies. Overall, we trust expertise. Bureaucracies are often the center of expertise on their respective topics by virtue of design and resources. For cybersecurity, most mature organizations still turn to their IT departments for solutions. Militaries, and their various armed services, are the bureaucracy experts: Generals are best equipped to manage armed conflict; Admirals would be the experts of choice in Naval warfare.

This straightforward confidence in expertise is fine when things are normal. Most would prefer that their problems be taken care by experts rather than visionaries. However, during periods of profound change, expertise may become an obstacle to adaptation. The philosophy and sociology of science - as well as empirical studies of organizational change in business and defense - explain why challenges to accepted views are more likely to come from sources outside the dominant system. Experts are those who have the strongest credentials under an existing paradigm, however, these also tend to be credentialed by a system that has arisen from the existing paradigm. That is, their status as experts is not independent of the theory, but is a product of the theory's success to date (Hill & Gerras, 2016).

As Thomas Kuhn writes:

Almost always the men who achieve these fundamental inventions of a new paradigm have been either very young or very new to the field whose paradigm they change (Kuhn, 1962).

Those we trust the most as experts are the least likely to recognize and identify anomalies, for the very reason that they are within the system. In armed forces, where the costs of failure can be catastrophic, bureaucracy is even less open to challenge. With experts who have not only professional authority, resources and prestige but also the power to command directly, the costs of subordinates questioning their expertise are prohibitive.

DOI: https://doi.org/10.5038/2378-0789.3.1.1039

Adversarial challenges coupled with misguided defense adaptation have repeatedly created conditions where defense has been rendered obsolete. The same situation has been unfolding in the last decade. In Table 1, a cyber RMA's catalyzing conditions are identified.

TABLE 1 THE CYBER-RMA SCENARIO

Newly possible method	Core competency rendered obsolete	Player affected
Destructive direct cyber-attack on strategic non-military homeland targets by foreign adversaries	**Defense**: perimeter protection, preventing enemy access to strategic targets at homeland **Deterrence**: establish attackers' identity to deliver punishment	All developed modern societies, with their respective defenses

A direct, destructive cyber-attack on civilian critical infrastructure breaks the fundamental strategic theory guiding every sovereign defense. As opposed to other types of attacks, cyber-attacks on computerized Industrial Control Systems (ICS) operating civilian critical infrastructure can reach strategic homeland targets without encountering nation-grade defenders. Foreign adversaries contemplating a destructive attack on a homeland target in a developed nation certainly face multiple state-run military-grade lines of defense on land, sea and air. This is in fact the main reason for the high level of security that citizens of Western countries enjoy: adversaries opt not to engage in warfare they are likely to lose.

However, cybered conflict has exposed a profound organizational vulnerability of westernized nations. It highlights the failure to produce a cyber RMA in order to defend as expected by the fundamental strategic theory of deterrence. At best, commercial-grade and profit-oriented technological solutions stand between a Stuxnet-like attack and homeland targets. Unlike most of history, militaries are not directly involved in protecting critical infrastructure or the homeland at large from strategic attacks. Foreign adversaries launching a direct, destructive cyber-attack on a non-military homeland target in the U.S. or Israel will not encounter defenses by the superior military forces. Armed forces do not shield society from cyber-attacks.

Moreover, the cyber attribution problem also profoundly undermines deterrence in the current socio-technical-economic system's architecture. While by no means is this attribution problem *inherent* in the technology, it is the result of architectural choices made in TCP/IP & Internet reinforced by market incentives. These inherent design characteristics are not easy to change. With the growth in the Internet of Things (IoT) and Industry 4.0, the attack surface available to adversaries expands, presenting even more lucrative targets and readily employedattack vectors.

Peacetime Strategic Maladaptation

Maladaptation almost never manifests in total unawareness of a changing reality, and western defenses are far from denying the major challenges of cyber. Militaries, intelligence and law enforcement agencies welcome the notion of adopting cyber technology to improve execution of existing strategies, increase efficiencies and improve core capabilities. How do armed forces today use their cyber warfare capabilities? Defense organizations universally do their own cybersecurity: namely, protect their own existing assets and capabilities. Each of the military branches knows what it does, and is determined to continue to do those things with help of new technology. This is tactical defense adaptation to cyber.

In militaries, as in any other professional bureaucracy or knowledge discipline, experts are accustomed to the existing fundamentals. Experts naturalize the rules of the game so that these fundamentals are removed from the scope of debate. Within professional communities - in science and in defense - experts are repeatedly taught the core professional principles throughout their career development. The core principles that lie at the heart of their theories become deeply embedded into the dominant paradigm, akin to axioms or laws of nature, never to be questioned. To challenge the core principles that lie at the heart of our theories is no simple task; to do so induces stiff expert opposition. The difficulty is that a profound change requires such a challenge.

One typical challenge is a war - a natural test that exposes many likely surprising obstacles and the risks of suffering a loss. Clearly, this is not a good option for U.S. or Israeli stakeholders. Another and less painful type of challenge emerges from intellectual and political efforts external to the military and outside of war, perhaps in efforts to avoid one.. For the purpose of this paper, a bird's eye overview of three peacetime strategic maladaptation cases will suffice to illustrate the

weight of internal expertise in preventing paradigm shifts. Among the telling cases which military innovation scholars have analyzed are the U.S. Army aviation revival, the Royal Navy failure to protect commercial shipping, and the IDF's initial refusal to adopt nontraditional responses to the rocket threat to Israel. (Griffin, 2017). For the example of civilian-led challenge and then adaptation, I turn to develop an additional recent case study: Israel Defense Forces' doctrine versus short-range rockets and missiles.

U.S. Army aviation revival after World War II

During its formation as a stand-alone service in 1947, the U.S. Air Force (USAF) aggressively argued for a central role in winning the next war by declaring its strategic application of airpower couldwin the war by itself. The USAF possessed institutional and professional expertise, a certain degree of institutionalized independence, and the freedom to build the forces in accordance with its own vision.

The U.S. Army, however, required air support for most of its land missions. The mandate to operate aerial power, as well as the capability, now rested with the USAF in managing the dissonance between two different missions, force structures, organizations and capabilities, the USAF mostly renounced the need to fly combat support missions for the Army. The US Department of Defense (DOD), which houses the civilian oversight of the Armed Forces, was unable to optimize the Air Force's role as the single air service across the services.

In particular, the U.S. Army engaged in elaborate forms of resistance, culminating in a very peculiar outcome. Eventually, in direct denial of the top-level political decision for USAF "owning" the air domain, the Army was able to acquire, operate, and maintain its own parallel air force (Bergerson, 1978). While fix-winged aircraft remained a USAF monopoly, the U.S. Army developed rotary-wing aerial firepower, i.e. helicopters armed with guns, rockets, and missiles (Bradin, 1994).

In this case, the Army's achievements show how sustained actions of "bureaucratic insurgents" – activist reformers who oppose policy yet work to change it from inside the organization – can produce highly disrupting results. In current context, the point here is that the USAF - as an armed forces branch owning a domain - was able to decide what defense roles it would not play. Its assumption of expertise and disdain of contrary paradigms left the other service

to scramble to meet the otherwise abandoned close air support needs from the domain it technically did not 'own' nor had expertise.. The USAF position was legitimated in large part due to the paradigm its experts held about what an Air Force did and did not do

Royal Navy Failure to Protect Commercial Shipping in WWI and WWII

The Royal Navy long enjoyed dominance of the world's ocean. The credit for its past success cemented the Navy's expertise in maritime defense. Unrestricted submarine warfare against commercial shipping was a very serious threat strategic to Britain in WWII. The German U-Boat threat already manifested on a smaller scale in WWI: U-Boats exposed the vulnerability of merchant shipping, on which the UK economy depended. In fact, U-Boats caused damages exceeded the Navy's expectations in WWI. (Herwig, 1996)

The UK antisubmarine division of the naval staff did analyze the submarine experience from World War I. Its findings appeared in a technical history series shortly after 1918. Yet the Admiralty classified the volumes, making them inaccessible to most officers rising through the ranks; moreover, in 1939 it then declared them obsolete and destroyed them. Advocacy for antisubmarine warfare often resulted in the termination of one's career. Britain's naval doctrine, developed largely by the Admiralty experts, resisted changes requiring the shifting of resources to counter U-Boats. Traditional service beliefs operated against learning the lessons of I9I7-I9I8. The Royal Navy discounted the submarine menace and passed the threat on to the air staff for resolution. But the Royal Air Force (RAF), which had control of virtually all air assets throughout the interwar period, proved even more disinterested in antisubmarine warfare at high sea (Herwig, 1996). In retrospect, air power advocates grossly exaggerated the airplane's role as a submarine killer. Royal Navy stubborn tenacity not to protect British merchant shipping is another example of a branch of armed forces owning a domain, and cherry-picking what parts of that domain it will accept as its responsibility.

In Kuhn's terms, submarine warfare against commercial shipping was an anomaly that normal science (which gave primacy to surface vessels) could not explain. The established Royal Navy bureaucracy used its weight of expertise to keep its preferred vision of victory and doctrine tied to battleships and major fleet engagements, costing the nation extraordinary amounts of lives and treasures when the war began.

Moreover, this maladaptation was not exclusively British. Between the World Wars, the navies of Britain, Germany and the U.S. all disregarded convoy protection and antisubmarine work.

> *In terms of an overarching doctrinal framework, the major naval establishments were united in the belief that submarines could never constitute true sea power and exercise either sea control or sea denial. This staunch orthodoxy worked to block innovation* (Herwig, 1996).

Israel's doctrine versus short-range rockets and missiles

Since 1969, the short-range rocket threat to Israel's homeland from the Northern border has been persistent. In 2001, it also materialized from the Gaza Strip in the South.[7] As most of these rocket attacks caused no significant damage, the IDF routinely disregarded the strategic and psychological aspects. While the military effectiveness of this threat was low in comparison with other kinetic options, it markedly showed that the IDF did not protect the homeland. From the 1970's to the 2000's, the IDF was drawn into recurrent conventional military operations to "purge" areas from rockets and thus to protect the nation from the short-range rocket threat.

Arguably, the recurrent IDF missions had operational success. But they also incurred heavy strategic costs. The 1982 Operation Peace for Galilee escalated into the First Lebanon War [8] The IDF's 1985 withdrawal to a Security Zone - and the subsequent military occupation of South Lebanon to create a buffer zone - exerted a heavy toll on Israel. The rise of Hezbollah and Shi'a dominance in South Lebanon cannot be explained and understood without examining the First Lebanon War. The IDF's May 2000 unilateral withdrawal from Lebanon and the collapse of the Lebanese Christian South Lebanese Army may have signaled a certain weakness in Israel's willingness to defend itself.

With the IDF playing a dominant role in Israel's security policy, the military experts chose to disregard the "flying tubes." The IDF contributed to overconfidence in Israel's deterrent. One senior expert demonstrated the mindset proclaiming Hezbollah's rocket arsenal will "rust" in

[7] As most of these did no material damage, the strategic and psychological aspects were routinely disregarded by the IDF.

[8] It started in large part to prevent bombardment on citizens of Northern Israel. The official Operation Peace for Galilee goal was to push the threat beyond the effective rocket range of 40 kilometers.

Lebanon warehouses.[9] This determined the low priority in developing countermeasures and investing in home front resilience, at the expense of restructuring military units. The four major IDF operations in the Gaza Strip between 2008 and 2014 led to a further erosion in public confidence and caused major domestic political changes in Israel.

Towards a Cyber Defense Paradigm Shift and RMA

To achieve national cyber security, one must challenge the established defense assumptions that have been formed as a result of centuries of war experience promoting particular paradigms in strategic defense adaptation. To succeed means a paradigm shift in defense, ie, a revolution in military affairs. How can we make this happen? A central finding of theoretical and empirical research is that threat awareness and the availability of technology are insufficient to drive an RMA. Technology enables the change: it sets the parameters of the possible, but cannot determine the exact type, direction and pace of change. Peacetime *strategic* defense maladaptation often does not stem from a lack of technology; rather it occurs because defense organizations are not willing to, not forced to, or not able to truly change their ways.

> *One of the most serious impediments to effective adaptation is that bureaucracies do not exist for the purpose of adapting to a changing and uncertain world. In fact, most bureaucracies oppose change, because it represents a direct threat to their position. Military bureaucracies proved absolutely necessary for the functioning of military institutions, but at the same time they have more often than not proved the enemy of innovation in peacetime* (Murray, 2011).

Military disasters are great promoters of defense change, but we would rather avoid this route. The civil-military model developed by Posen in the early 1980's concludes that interwar (i.e. "peacetime") military innovation will only occur if civilian statesmen intervene in the development of military service doctrine, preferably with the assistance of maverick officers[10] from within the service (Posen, 1984). Peacetime innovation requires military allies. Other researchers (Cote, 1996) have argued that civilian leaders can leverage and "manipulate inter-service competition to cause doctrinal innovation," i.e. peacetime strategic innovation. However,

[9] Ari Shavit interview with former chief of staff Moshe Ya'alon Sep 14, 2006 Haaretz, https://www.haaretz.com/no-way-to-go-to-war-1.197210

[10] Officers with unconventional ideas who are willing to cooperate with civilians to reshape the military.

outside leaders are unlikely to impose a new vision of future war on a military service that is committed to ways of fighting in which it excels. The complexity of modern military bureaucracy suggests that one or two vocal visionaries will not penetrate the silos and will not drive revolution in military concept and doctrine.

However, the expectation of military failure assists civilian impact on militaries. A stark demonstration of technology or method producing severe damage allows outsiders to challenge the relevance of defense expertise. Outside leaders could assist these efforts by supporting organizations testing visions of future war, experiments that create, examine and disseminate empirical evidence for the need to change. To shed light on successful innovations, I turn to discuss Israel's path to the Iron Dome.

National security: Iron Dome as a defense adaptation success

Despite the high political cost of military response and the economic/morale damage caused by bombardment, the Israel Air Force (IAF) - responsible for air defense - opposed the idea that short-range projectiles deserve interception. Then-IDF chief of staff Air Force Major-General Halutz said that short-range imprecise and small rockets are not a decisive weapon (Shelah, Limor, & Kats, 2007). This was technically correct. The IAF doctrine relied on superior intelligence and precision strike capabilities. This not only enables to destroy larger launchers, but also to enhance deterrence, including by decapitation. The main arguments against intercepting the rockets were that it was strategically unwise, technically impossible[11], and prohibitively expensive.

In the summer of 2006, Hezbollah attacked a military patrol in Israel, killing three and abducting two Israeli soldiers. In response, Israel launched a military operation in Lebanon. The IAF indeed swiftly destroyed 59 intermediate and long-range missile launchers in the Hezbollah arsenal, in a long-planned and well-executed raid (Lambeth, 2011).[12] However, as the IDF knew well before 2006, the shorter-range rockets that do not require installations could not be neutralized from the air. Over the 33 days of the Second Lebanon War, Hezbollah fired more than 4,200 rockets into northern Israel, killing 44 Israelis. The fact that Hezbollah kept up its daily bombardment was the main cause of broad popular frustration. A quarter of the short-range

[11] Israel already was the most advanced state in active ballistic missile defense (BMD) in the region at least since mid-1990s, with excellent technical expertise.
[12] http://www.ynet.co.il/articles/0,7340,L-4827205,00.html

Katyusha rockets launched hit urban areas, paralyzing Northern Israel - especially the main port of Haifa, refineries and many other strategic installations (Rubin, 2007). The strategic and political results of the war were poor, resulting in the removal of the Prime Minister and IDF Chief of Staff from office, and a profound political upheaval.

Despite the Israeli outcry over the IDF's failure to achieve a clear-cut victory (Kober, 2008), Hezbollah has refrained from launching rockets to Israel for over a decade, which suggests deterrence (Sobelman, 2017). However, Palestinian militants in the Gaza Strip (that came under Hamas control) emulated the rocket strategy.[13] Short-range rockets were not a decisive weapon, but as Hamas improved its capabilities, more Israeli cities (including *Sderot*, and later *Ashkelon*, *Ashdod* and *Be'er Sheva)* came under persistent rocket attacks from Gaza. These spurred several IDF operations against Hamas in the Gaza Strip.[14]

Nevertheless, the IDF and most of the defense establishment continued to hold the doctrine of deterrence by punishment and taking the fight to enemy territory. Particularly disconcerting was the denial of the need to protect the homeland better. Active defense was not accepted because it constituted a strategic doctrinal reversal from offense and deterrence to protection and resilience. By 2011, Hamas grew able to launch missiles to Tel Aviv despite two major IDF operations as well as leadership decapitations.

In 2004, then-Brig. Gen. Daniel Gold was named Director of the Ministry of Defense's Research and Development department (MAFAT), responsible for overseeing the development of new weapons systems. MAFAT has the authority to invest in areas without a requirement by the IDF services or arms. Gen. Gold took up the rocket challenge, which the IDF still mostly considered as secondary. In 2005, MAFAT put out a request to defense companies to propose anti-rocket systems, a call that eventually led to the development of the "Iron Dome" concept. In 2007, Israel commissioned the development of Iron Dome, choosing the Israeli company Rafael as key developer. The IDF did not support the effort.

[13] It hardly came as a surprise: fictional "Rockets on Ashkelon power production plant" threat featured in political campaigns opposing the Oslo Accords in the early 1990s. The first Hamas-fired Palestinian rocket hit Israel in early 2001. In 2005, before the Second Lebanon War, Hamas fired 1,200 rockets https://www.idfblog.com/facts-figures/rocket-attacks-toward-israel/ .

[14] Operation "Hot Winter" launched on February 29, 2008; Operation "Cast Lead" launched on December 27, 2008; Operation Pillar of Defense launched on November 14, 2012; and Operation Protective Edge launched on July 7, 2014.

Then-Minister of Defense Amir Peretz was an outsider: the rare civilian defense minister with no military background or experience. Peretz is also from *Sderot*, the southern Israeli town that endured high-volume Palestinian rocket fire for many years. In August 2006, Gen. Gold and his team briefed the Minister on Iron Dome. After the Second Lebanon War, military experts could no longer could dismiss the threat. Those who still could dismiss its significance would think twice before telling so to the Minister with a personal experience of seeking shelter in 15 seconds. Nonetheless, all military experts slammed the Iron Dome concept, attacking Peretz personally and attempting to leverage his lack of defense expertise against him on this concept. However, in early 2007, Peretz threw his full ministerial weight behind the project, committing another $10 million in Ministry of Defense funds to keep the project alive. Peretz did so without military or government approval.

The Iron Dome air defense system went from the drawing board to combat readiness in less than four years, placed with the IAF air defense and declared operational in March 2011. It has proven combat success in Israel's unique circumstances (Dombrowski, Kelleher, & Auner, 2013). According to the Israeli Air Force, during the November 2012 seven-day Operation Pillar of Defense, Iron Dome made 421 interceptions.On November 17th, after two rockets surprisingly targeted Tel Aviv, a battery was deployed in the area. Within hours, the system intercepted a third rocket. During the 51 days of Operation Protective Edge in 2014, Palestinian militants in the Gaza Strip launched some 4,200 rockets, of which 3,417 landed in open areas, 224 hit urban zones including Tel Aviv and Jerusalem, and 735 were intercepted by Iron Dome (Eilam, 2016).

The Iron Dome story provides support for the civil-military model of military innovation that is missing in today's adaptations to the homeland cyber threats. The political efforts of the civilian Minister of Defense Amir Peretz, in conjunction with Gen. Gold, a strong MoD ally in MAFAT who also happened to be an IAF officer, are what made Iron Dome real. Gen. Gold was the military visionary champion of change, while Peretz was the rare outsider in the Minister of Defense post, a civilian force. Working together, they succeeded in imposing a profound strategic change in Israel's defense strategy, doctrine, force build-up, resource allocation and operations. Moreover, despite the obvious value of defending the civilian population against intermittent short-range rocket barrages, the decision to defend actively was made and implemented against the will of the IDF general staff, the IAF air defense leaders, and most security experts. The fact that the Iron Dome active missile defense system was developed and fielded epitomizes successful defense

adaptation. It also is a strong example of the difficulties that strategic defense adaptation needs to overcome. Future research can use this case to explore the validity of military innovation models (Grissom, 2006)

The civil-military military innovation model argues that peacetime military innovation occurs if civilians intervene in military service doctrinal development, preferably with the assistance of maverick officers from within the service (Posen, 1984). Both the civilian top-down intervention (Peretz) and the military champion of change (Gold) were driving forces in Iron Dome. Additionally, the Inter-Service Military Innovation model suggests that more such initiatives are to be expected. In pursuit of now-lucrative homeland defense missions against lower-intensity threats, land forces, artillery corps and infantry are likely to promote alternative tactics and platforms to counter the short-range rocket threat.

Conclusion

This analysis spells trouble for the U.S. and its allies. Armed forces, intelligence organizations and defense ministries have amassed the most advanced and substantial cyber warfare capabilities and capacities**.** Nevertheless, ministries of defense and armed forces are, at best, bystanders in national cyber defense; they only marginally assist in defending homeland critical targets. The endgame is that, asforeign adversaries wage cybered conflict inflicting significant economic and social toll at the homeland, their appetites and arrogance are growing.

The Western failure in peacetime strategic defense adaptation – by the armed forces in particular – is the underlying cause of this profound strategic anomaly. A direct, destructive cyber-attack on civilian critical infrastructure violates the fundamental strategic theory guiding every sovereign defense. In fact, all branches of armed forces are sticking to their guns, embracing cyber technology only for existing missions, and leaving their sovereign defense responsibilities unfulfilled in a cybered threat rich world.

Cybered conflict demands new missions, doctrine and force structure, at the expense of older ones. Simply seeking and deploying more sophisticated technology within existing organizations will not improve security. Models of defense adaptation stress the importance of political and organizational aspects. But maladaptation occurs because defense organizations are

either not willing to, not forced to, or not able to change. The role of expertise is significant. Generals often uphold a common and dated cyber defense position: armed forces cannot be responsible for defending society from cyber-attacks on strategic non-military homeland targets by foreign adversaries. They argue that national cybersecurity practices are incompatible with the established authority, structure, and ways of practice of armed forces. The expert's analysis of the past ways and established practices of warfighting are taken to be correct. Indeed, a common slippery slope argument is that democratic societies should not accept defense at the presumed cost of militarization of domestic affairs and erosion of basic freedoms.

But what if the core capabilities for defending society in cybered conflicts differ from the past? Would defense organizations and their experts be able to recognize it, and lead a radical adaptation that retires much of their cherished traditions and endangers their expertise? Security Studies theory, philosophy of science, and empirical evidence all suggest that profound defense adaptation demands external pressure on the expert organization. The recent Iron Dome case study shows that civilian outsider pressure and insider champions of change within the military are both necessary for strategic adaptation. In both the US and in Israel, insufficient challenge to the established paradigm is hindering the necessary development of a cyber RMA. This analysis may help military and civilian stakeholders to drastically improve national cyber security instead of waiting for the losses of war to force true RMA adaptations.

REFERENCES

(U.S.)., N. R. C., Board., C. S. a. T., & System Security Study Committee. (1991). *Computers at risk : safe computing in the information age*. Washington, D.C.: National Academy Press.

Bergerson, F. A. (1978). *The Army gets an air force : tactics of insurgent bureaucratic politics*. Baltimore: Johns Hopkins Univ. Pr.

Bradin, J. W. (1994). *From hot air to hellfire : the history of army attack aviation*. Novato, CA: Presidio.

Brenner, J., & Lindsay, J. R. (2015). Correspondence: Debating the Chinese Cyber Threat. *International Security, 40*(1), 191-195. doi:10.1162/ISEC_c_00208

Cheung, T. M. (2009). Dragon on the Horizon: China's Defence Industrial Renaissance. *Journal of Strategic Studies, 32*(29-66).

Cote, O. R. (1996). *The politics of innovative military doctrine : the U.S. Navy and fleet ballistic missiles.* Retrieved from http://dspace.mit.edu/handle/1721.1/11217 Available from http://worldcat.org /z-wcorg/ database.

Demchak, C. C., & Dombrowski, P. (2011). *Rise of a Cybered Westphalian Age*. Ft. Belvoir: Air Univ Maxwell Afb Al Defense Technical Information Center.

Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet, 4*(3), 672-687.

Dombrowski, P., Kelleher, C., & Auner, E. (2013). Demystifying Iron Dome. *The National Interest*(126), 49-59.

Eilam, E. (2016). The Struggle against Hizbullah and Hamas: Israel's Next Hybrid War. *Israel Journal of Foreign Affairs, 10*(2), 247-255. doi:10.1080/23739770.2016.1207130

Griffin, S. (2017). Military Innovation Studies: Multidisciplinary or Lacking Discipline? *Journal of Strategic Studies, 40*(1-2), 196-224. doi:10.1080/01402390.2016.1196358

Grissom, A. (2006). The future of military innovation studies. *Journal of Strategic Studies, 29*(5), 905-934. doi:10.1080/01402390600901067

Herwig, H. H. (1996). Innovation ignored: the submarine problem—Germany, Britain, and the United States, 1919–1939. *Military Innovation in the Interwar Period*, 227-264.

Hill, A., & Gerras, S. (2016). Systems of Denial. *Naval War College Review, 69*(1).

Hundley, R. O. (1999). Past revolutions, future transformations what can the history of revolutions in military affairs tell us about transforming the U.S. military? *United States Defense Advanced Research Projects Agency National Defense Research Institute Rand Corporation.* Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=20495

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA364037

Kober, A. (2008). The Israel defense forces in the Second Lebanon War: Why the poor performance? *Journal of Strategic Studies, 31*(1), 3-40.

Kragh, M., & Åsberg, S. (2017). Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal of Strategic Studies*, 1-44. doi:10.1080/01402390.2016.1273830

Kramer, F. D., & Wentz, L. K. (2008). *Cyber influence and international security*. In Defense horizons, Vol. 61. Retrieved from http://purl.access.gpo.gov/GPO/LPS105624

Kuhn, T. S. (1962). *The structure of scientific revoutions*. Chicago: The University of Chicago Press.

Lambeth, B. S. (2011). Air operations in Israel's war against Hezbollah learning from Lebanon and getting it right in Gaza. *Project Air Force.* Retrieved from http://www.books24x7.com/marc.asp?bookid=58308

McConnell, M., Chertoff, M., & Lynn, W. (2012, January 27). China's Cyber Thievery Is National Policy-And Must Be Challenged *The Wall Street Journal*.

Murray, W. (2011). *Military adaptation in war : with fear of change*. New York: Cambridge University Press.

Posen, B. (1984). *The sources of military doctrine : France, Britain, and Germany between the world wars*. Ithaca: Cornell University Press.

Rubin, U. (2007). *The rocket campaign against Israel during the 2006 Lebanon War*: Begin-Sadat Center for Strategic Studies, Bar-Ilan University.

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies, 40*(7), 898-926. doi:10.1080/01402390.2017.1307741

Shelah, O., Limor, Y., & Kats, I. (2007). *Shevuyim bi-Levanon : ha-emet `al milhemet Levanon ha-sheniyah* | שבויים בלבנון : האמת על מלחמה לבנון השנייה. Tel-Aviv: Yedi`ot aharonot : Sifre hemed | ידיעות אחרונות : ספרי חמד.

Sobelman, D. (2017). Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–16. *International Security, 41*(3), 151-196.

Tabansky, L. (2013). Critical Infrastructure Protection Policy: the Israeli Experience. *Journal of Information Warfare, 12*(3).

Tabansky, L. (2017). Cybered Influence Operations: towards a scientific research agenda. *Security Policy Library - The Norwegian Atlantic Comittee, 2017*(2), 36.

The Australian Strategic Policy, I. (2015). When states strike backnational responses to cyber incidents. *The ASPI Strategist*, 2015-2008.

Verizon report shows business is booming for cyber-criminals. (2017). *Computer Fraud & Security, 2017*(5), 1-3. doi:https://doi.org/10.1016/S1361-3723(17)30036-2

Zetter, K. (2014). *Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon*. New York: Crown.