CYBER POWER IN THE CHANGING MIDDLE EAST

The turmoil that characterized the ruins of the century-old colonial Sykes-Picot order undermined the security environment for Ankara and Jerusalem alike. The geopolitical great power conflict will unfold turbulently in what was Syria and Iraq. Concurrently, cyber technology provides actors with new tools to achieve the desired effect and gain power. Israel has allegedly utilized original cyber power for strategic purposes in Syria and Iran. Russia, now entrenched in Syria, has created cyber power and has been effectively using it for a long time. In this article, the author argues that in order to remain a pivotal regional power, Turkey must drastically boost its sovereign cyber security. Given Turkey's deteriorating security environment, its strained bilateral relations with Israel and the US, and especially the escalation risk in tensions with Russia, Turkey will be hard pressed to drastically bolster its sovereign national cyber security on its own.

Lior Tabansky[*]

TURKISH POLICY
QUARTERLY
Spring 2016

[*] Lior Tabansky is a researcher at the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University (TAU), a PhD candidate in the School of Political Science at TAU, and Director of Strategy for Cyber Security Group consultancy.

Cyberspace is a man-made environment; it can be disassembled, remodelled, and perhaps destroyed, at least temporarily and within spatial limits. “Cyber war” is a common term, but it generally misleads more than it illuminates. Professor Chris C. Demchak of the US Naval War College introduced the term “cybered conflict.”[1] It is a much more appropriate term because it underscores the omnipresence of cyber technology in every sphere of activity, including conflict. Cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.[2] Cyber power debates must focus on the deep, complex, and intimate integration of cyber technology across public and private systems, across sectors from media and the economy to defense, and across all key societal functions. The accumulated experience suggests that attackers have the advantage in cyberspace. Therefore, incentives for state-sponsored actors to obtain and exploit capabilities are likely to rise. International relations and strategic studies scholars today should theorize about the nature of cybered interstate conflict.

The century-old colonial Sykes-Picot legacy has been a disaster for many people in the greater Middle East. In recent years, the unravelling of many artificial undemocratic states has spawned multiple non-state actors, resulting in violence and suffering for the people in the region. Ungoverned territories in Syria and Iraq are likely to remain one of the focal points in these complex sectarian conflicts. However, Syria and Iraq have also become a scene of great power conflict.

Russia Revisits the Region

Russia’s systematic strategic efforts to expand and enhance its presence in the Middle East have borne fruit. Russia has gained the lasting position of influence it has sought for decades. Since August 2015, Russia’s bold and prompt moves in Syria have dramatically shifted the global balance of power, and directly, albeit differently, impacted the strategic environment for both Turkey and Israel. Cyberspace plays a prominent role in Russia’s strategic and doctrinal writing on (inter)national security.[3] Given the scope of this article, the following discussion will only present a recent cyber attack attributed to Russia.

[1] Chris Demchak, “Cybered conflict, cyber power, and security resilience as strategy,” *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S Reveron, (Georgetown: Georgetown University Press, 2012), p. 121-136.

[2] Daniel Kuehl “Cyberspace and Cyberpower” in Franklin Kramer, Stuart Starr, and Larry Wentz (eds.), Cyberpower and National Security (National Defense University Press, 2009).

[3] Oleg Demidov, “Cyberwarfare and Russian Style of Cyberdefense,” *Security Index: A Russian Journal. on International Security*, Vol. 19, No. 3, (September 2013), p. 67-71.

Ukrainian Regional Electricity Distribution

On 23 December 2015, Ukrainian regional electricity distribution companies experienced unscheduled service outages in multiple central and regional facilities. The company in the Kiev region told customers that the outages were due to a third party's illegal entry into the company's computer and SCADA systems. Originally thought to have affected approximately 80,000 customers, it was revealed that several outages caused approximately 225,000 customers to lose power across various areas. According to US-led investigations, these outages were caused by synchronized and coordinated remote cyber attacks.[4]

Cyber attacks were executed at three regional electric power distribution companies within 30 minutes of each other, via either existing remote administration tools at the operating system level or remote Industrial Control System (ICS) client software using Virtual Private Network (VPN) connections. The attackers employed spear-phishing emails, corrupt Microsoft Office documents, and variants of the BlackEnergy 3 malware, to gain and sustain a foothold in the corporate networks of the electricity companies. This was done to harvest credentials and information to access the ICS network.[5] In one case, the attackers generated thousands of calls to the energy company's call center to deny access to customers.

> *"Cyberspace is a man-made environment; it can be disassembled, remodelled, and perhaps destroyed, at least temporarily and within spatial limits."*

These capabilities are actually widely available in the criminal market.[6] The attackers knew the exact operation of the ICS, which is a significant fact in terms of attributing the origin of the attack. They overrode several safety mechanisms to achieve their malicious effect, including server Uninterruptable Power Supplies (UPSs), and the Human Machine Interface (HMI) operators used to monitor ICS.

[4] The U.S. Department of Homeland Security (DHS) issued a formal report on February 25, 2016. An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/ Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
See also: (Assante, Conway, and Lee, (2016).

[5] Michael Assante, Tim Conway, and Robert M Lee, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, E-ISAC: E-ISAC, SANS-ICS, (2016).

[6] Lior Tabansky, "Cybercrime: A National Security Issue?", *Military and Strategic Affairs*, Vol. 4, No. 3 (December 2012), p. 117-136.

They targeted field devices at substations, which are hardly an area of expertise among common hackers. To deepen and prolong the effect, the attackers wrote custom malicious firmware, delivered it via the network to field devices such as Serial-to-Ethernet devices at substations, thus rendering industrial equipment inoperable and largely unrecoverable.[7]

> *"Cyberspace plays a prominent role in Russia's strategic and doctrinal writing on (inter)national security."*

While the Ukrainian Security Service (SBU) and the international press were quick to blame Russian state-backed hackers, Moscow has remained silent. It was safe to do so: the nature of cyber warfare makes it almost impossible to discover the operator from technical evidence. This is referred to as the "attribution problem."[8] However, the attackers demonstrated the ability to perform the long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multi-stage, multi-site attack. These, and the targets chosen, suggest a political, not criminal motivation.

Israel and Cyber Power

Since the 1977 Israel-Egypt Peace Agreement, the risk of massive military invasion from neighboring Arab countries has diminished. The subsequent sustained deterrence of Bashar al-Assad's Syria since 1982, the 1994 peace agreement with Jordan, the removal of Saddam Hussein's regime as well as ties with Turkey, all improved Israel's security, but other threats have emerged. On the one hand, armed non-state organizations such as Hezbollah, Hamas, and Islamic Jihad present a lower intensity threat, i.e. something less than a full-scale war. On the other hand, the Islamic Republic of Iran, who is neither Arab nor a neighbor of Israel, poses an imminent nuclear threat. The prospect of nuclear weapons in the hands of hostile radical regimes is the top strategic threat to Israel. To prevent hostile nuclear programs, Israel has consistently been willing to unilaterally resort to military force, including destructive aerial strikes on Iraq's Osiraq in 1981 and Syria's al Kibar in 2007.[9]

[7] Firmware is the combination of persistent memory and program code and data stored in Hardware.

[8] Jon Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," *Journal of Cybersecurity*, Vol. 1, No. 1 (November 2015), p. 53-67; Ben Buchanan and Thomas Rid, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol. 1, No. 43 (December 2014).

[9] Austin Long and Whitney Raas, "Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities," *International Security,* Vol. 31, No. 4 (2007), p. 7-33; Amy Butler, David Fulghum, and Robert Wall, "Israel Shows Electronic Prowess," *Aviation Week and Space Technology,* Vol. 168, No. 25 (2007).

But the destructive cyber attack on Iran's Natanz fuel enrichment program (FEP), discovered in 2010, was the first of its kind and is certainly a harbinger of the future.

Operation Olympic Games

Because the radical Iranian revolutionary regime consistently declares its desire to destroy Israel, the Iranian nuclear program has topped Israeli threat assessments for decades. The program's key industrial component is the FEP – the largest gas centrifuge uranium enrichment facility in Iran. The FEP has three large buildings totalling 100,000 square meters. It is built eight meters underground and protected by a concrete wall 2.5 meters thick, which is itself protected by another concrete wall and buried under a layer of earth. Two of the three buildings are cascade halls built to hold up to 50,000 centrifuges, which in full capacity can enrich uranium for some 20 bombs annually. The international non-proliferation regime failed to stop the Iranian nuclear program. Diplomatic efforts to curtail the program suffered a blow with the election of the conservative President Mahmoud Ahmadinejad in August 2005. On 10 January 2006, Iran broke the seals safeguarding FEP and resumed its enrichment program; the FEP was fully operational by February 2007, in contravention of UN Security Council resolutions demanding Iran halt its uranium enrichment.

> *"In 2014, Israeli companies sold around six billion dollars of cyber security solutions. This amounts to almost 10 percent of the global cyber security market."*

The discovery of Stuxnet malware in July 2010 was an eye-opener for the public. The sophistication of the targeting, delivery, detection evasion, and most of all the destructive payload were all unprecedented. The malware was written to compromise a Microsoft Windows computer, then infiltrate and propagate inside corporate air-gapped networks, to seek and silently disrupt a specific Industrial Control System (ICS).[10] Versions of the malware were probably installed in late 2007 and 2009. By the end of 2010, the worm had infected approximately 100,000 hosts in dozens of countries, 60 percent of which were in Iran.[11] The malware propagated in at least seven ways, but the infection did no damage. Stuxnet is a precision-guided cyber weapon. Stuxnet seeks a specific hardware and software configuration of Siemens-made WinCC/PCS 7

[10] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival,* Vol. 53, No. 1, (2011) p. 23-40; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

[11] Zetter (2014).

"As the concepts have been validated and states are learning, cyber warfare is likely to increase within interstate conflict contexts."

supervisory control and data acquisition (SCADA) software[12] with two models of Siemens-made programmable logic controllers (PLC), 6ES7-315-2 and 6ES7-417.[13] Only when the specific configuration is found does the malware activate the weaponized payload. Stuxnet did not shut down the targeted system, but instead temporarily reprogrammed SCADA system's human – machine interface (HMI) output, to display activity as normal and suppress alarms.[14] Before Stuxnet started sabotaging ongoing processes, it intercepted input values from sensors – for example, the state of a valve or operating temperatures – recorded these data, and then provided the legitimate controller code with pre-recorded input signals, while the malware manipulated actual processes in the background.[15] It damaged the uranium enrichment process at the Natanz FEP by covertly reprogramming the PLC controlling the centrifuges to periodically spin the motor out of the safe range, disrupting enrichment and eventually causing malfunction and physical destruction of about 1,000 out of the 9,000 IR-1 centrifuges deployed at Natanz in late 2009.[16]

Soft Power Includes Most Non-Military Aspects Such As Exports

Israel has traditionally developed advanced technology for defense.[17] But the persistently high investment in Research and Development (R&D) – roughly double the OECD average – has also produced much larger spillover effects including nurturing human capital, competitiveness, and economic benefits. These are now evident in cyber security, which has enjoyed meteoric commercial growth. The three billion dollars of exports in 2013 doubled in 2014.[18] In 2014, Israeli companies sold around six billion dollars of cyber security solutions. This amounts to almost 10 percent of the global cyber security market, valued at 60 billion dollars in 2013 by the IT consultancy firm Gartner. For the first time in history, the total value of Israeli cyber security exports outpaced Israeli defense exports. The

[12] Zetter (2014).

[13] Ralph Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security and Privacy, IEEE,* Vol. 9, No. 3, (2011), p. 49-51.

[14] Yoaz Hendel and Yaakov Katz, *Israel vs. Iran: The Shadow War* (Washington, DC: Potomac, 2012).

[15] Langner (2011).

[16] Langner (2011).

[17] Ben-Israel and Tabansky (2015).

[18] "Cyber-boom or cyber-bubble? Internet security has become a bigger export earner than arms," *The Economist*, 2015.

dynamic innovation continues. The Israeli society produced some 300 cyber security start-ups in 2015, up from 150 in 2012.[19] In 2014, eight of them were sold to foreign investors, for a total of 700 million dollars. The Israeli National Cyber Bureau (INCB) estimates Israeli cyber security exports reached 3.5 billion dollars in 2015, about five percent of the global cyber security market valued now at 75 billion dollars. The nominal decrease is explained by foreign (mostly American) firms acquiring Israeli exporters, for a total of 1.3 billion dollars in 2015. The private sector is clearly an indispensable component of national cyber security.

The Future of Cybered Conflict in the Middle East

Until Stuxnet, sending bits of information to wreak direct physical damage was an experimental theory tested only in the laboratory. But in Operation Olympic Games, a cyber attack was chosen over available kinetic options and thrown into a battle of the highest strategic importance. Stuxnet demonstrated several major breakthroughs in cyber warfare:

- engage a high-end, protected, air-gapped target
- target discriminately and precisely
- stealthily cause sustained effects for prolonged periods
- physically destroy industrial equipment by software means alone

In the five years since the discovery of Stuxnet, most developed nations have worked out and implemented at least one national cyber security strategy. Despite the progress, the risk remains high. China has been blamed for massive industrial espionage. Russia has been blamed for cyber disruptions of critical infrastructure. The Islamic State of Iraq and the Levant (ISIL) is exploiting cyber space in multiple ways. The problem of attribution precludes many conventional defense options. As the concepts have been validated and states are learning, cyber warfare is likely to increase within interstate conflict contexts.

Israel has little ambition in the region beyond security. Neither the Israeli public or its leadership entertain any utopian illusions regarding the implosion of the Sykes-Picot order. Israel has formed two trilateral alignments, one between Greece, Israel, and Cyprus, and the other between Israel, Egypt, and Cyprus, in the Eastern Mediterranean. Israel has maintained peace with Egypt and Jordan. Israel's strategic interest remains twofold: averting the Iranian nuclear bomb and curbing violent Jihadist extremism.

[19] A start up can be defined as an "organization formed to search for a repeatable and scalable business model, typically technology oriented."

Implications for Turkey: The Mounting Need for Cybersecurity

Turkey has the geo-strategic potential to become a powerful regional actor. To fulfill this potential, capability must complement intent. Any serious assessment of Turkish foreign and security policy exceeds the purpose and scope of this article. One major change is evident even to non-experts. In the first decade of the 2000s, Turkey's foreign policy motto of "zero problems with neighbors" seemed a viable strategy. Ankara developed cordial relations with a broad range of players in the Middle East and North Africa (MENA) and offered mediating action to the region's conflicts, such as Israel-Palestine, Israel-Syria, Lebanon, and Iraq. Ankara pursued independent policy, such as close ties with Syria and Iran despite Washington's disapproval of such policies. Ankara's reluctance to normalize relations with Israel, despite the public apology by Israeli Prime Minister Netanyahu for the *Mavi Marmara* incident that President Obama personally brokered, soured relations with Washington as well. As cyber power becomes an essential instrument in international security, Turkey's cyber security deficiencies may prove crucial. Russian security thinking can be innovative, unpredictable, and effective. Moscow apparently now has the ability to fulfill longstanding ambitions. Recently, Russia has gained the lasting position of influence it has sought for decades. In Syria, Moscow backs Assad's forces, while Ankara supported the opposition. The interception of the Russian Air Force Su-24M by Turkish F-16s on 24 November 2015 has further strained Turkish-Russian relations. In light of this, it is safe to predict that the Turkish-Russian conflict will be a deeply "cybered" one.

Given Turkey's deteriorating security environment, its strained bilateral relations with Israel and the US, and especially the risk of escalation in tensions with Russia, Turkey will be hard pressed to make progress on its own.