Konrad Adenauer Stiftung

Mediterranean Advisory Group

Mediterranean Dialogue Series | No. 15

REGIONAL PROGRAM POLITICAL DIALOGUE SOUTH MEDITERRANEAN

CYBERED CONFLICT IN THE MIDDLE EAST

The following discussion paper is informed by debates at the *Mediterranean Advisory Group* meeting on "The Future of Middle Eastern Warfare" organized by the KAS Regional Program South Mediterranean from 26-27 April 2018 in Jerusalem.

Authors: Kristina Kausch & Lior Tabansky

Cyber power has a vast geopolitical potential. Cyber technology is increasingly inseparable from all instruments of power, including diplomacy, information, economy and military. International relations and strategic studies have traditionally emphasized the importance of geographic proximity for nature of interstate conflict. Cyber technology alters, and on occasions even obsoletes, the value of proximity in the geostrategic environment. This change demands a major conceptual shift in defense.

The Middle East remains a region in which local, regional and global geopolitical conflicts conflate. While cyber capacities in this region are still limited, recent years have seen a boost in the use of cyber power in old and new Middle Eastern conflicts. Existing political tensions and conflicts have gained an additional arena allowing for more rapid escalation. This conference paper summarises some of the challenges arising from cybered conflict in the Middle East and outlines possible trends.

Cybered Conflict: A Geopolitical Game-Changer?

The use of cyber power for geopolitical ends is no recent development. Before the first Gulf war, the US government hacked Iraqi officers' email accounts. Most operations today – such as the hacking of ISIS websites by the US government – remain below the radar of broader public perception. Yet technological advances, progressive digitalisation and interconnectivity have created vulnerabilities that have led to a boost of malicious cyber operations in recent years, including for commercial and geopolitical gain.

Cyber-attacks can be grouped in two types: breaches to gather and use information (Computer Network Exploitation, or CNE), and attacks on systems (Computer Network Attacks, or CNA) to block or damage adversaries' networks, such as of governmental bodies, symbolic targets, and critical infrastructure. Cyber operations impact at three interwoven levels: the physical, the digital, and the cognitive domain. Information warfare, for example, is increasingly carried out via cyber channels.

While defense is becoming gradually digitalized, cyber power must be assessed not isolated from other means of warfare but as one part of the combined arsenal at a state's disposal. In defense terms, the emergence of cyber can be seen as another alteration of battle space – from the ground to the seas to space, and eventually creating a new space, from which power is projected to the physical domain, too. In this new battle space, many classical defense concepts and terminology do not apply.

Cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.[1] "Cyber war" and "Cyber warfare" have become commonly used expressions. However, both focus on an ideal domain-confined construct and fail to illuminate the full breadth of technology-enabled potential. Chris C. Demchak of the US Naval War College has introduced the term "cybered conflict"[2], which underscores the omnipresence of cyber technology in all activity, including in conflict. Cybered conflict is therefore the appropriate term, rather than warfare, as it allows accommodating for the complex interactions between a broad variety of stakeholders, operations crosscutting distinct domains, and all activities short of armed conflict.

The opportunities and challenges inherent to cyber have led to calls for a comprehensive framework for global cyber governance. Ongoing efforts to build cyber governance focus on three pillars: overarching cyber norms (including the idea of applicability of cyber, and the impact of cyber on civilians during peace time); binding agreements (valid not only for states but that cannot be exploited by criminals and other non-state actors either, involving major tech companies to abound by those rules to protect users); and attribution (including avoiding single actor attribution leading to intentional or non-intentional misinterpretation of evidence).[3]

Cyber power is at times portrayed as the "perfect weapon". Combining disruptive potential and quick deployment at low political and economic cost, cyber attacks allow cheap, quick, global impact. The wide range of possibilities, the delay in defense response, and the ease of participation for a much wider range of non-state actors, all contribute to this impression. However, uncertainties in the use of cyber power, including a lack of control over the result and consequence of attacks, significantly reduce its targeted use. Moreover, the difficulty for most aspiring cyber actors of developing large impact capacities currently make cyber an enabler rather than a full-fledged geopolitical game changer.

Many questions remain unanswered: is the future of warfare micro targeting or massive attacks? How can we measure cyber capabilities? Can we predict, discriminate, and localize effects of attacks at a time when almost everybody can participate in the game? How can geography be projected in cyberspace? Particularly relevant to cyber's geopolitical meaning is its impact on deterrence.

[1] Daniel T Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," ed. Franklin D. Kramer, Larry K. Wentz, and Stuart H. Starr, *Cyberpower and national security* (Washington, D.C.: National Defense University Press : Potomac Books, 2009), http://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

[2] Chris C. Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (2012).

[3] See also Peter Chase, Bruno Lété: Shaping responsible behavior in cyberspace, GMFUS, 28 June 2018.

Does Cyber Erode Deterrence?

Incorporating non-conventional means of warfare, including cyber, into traditional defense structures and approaches is a major policy challenge. It has been argued that cyber can change geopolitical calculus in relation to traditional forms of power projection, notably eroding mechanisms of deterrence. Experts have widely debated the attribution problem in cyber and the challenges it presents to deterrence. Deterrence works by convincing one's adversary that the costs of conducting an attack outweigh potential benefits, and a precondition for this is attribution. Mature cyber security can acquire the ability to identify the attacker, but very few cyber actors can rely on such mature systems, so the attribution of cyber attacks is mostly a matter of capacity. Without the capacity for attribution there can be no effective defense, and even among the most advanced economies, few governments (for example the United States, the United Kingdom, but not Germany) currently have such mature capacity. International standards of proof for attribution are an ongoing debate in international law, and lest are there any such standards for offenses committed in cyberspace.

The blurring lines between threat actors in cyber complicates attribution even further. Nations make a distinction between the forces defending from external attack (militaries) and those protecting law and order inside the nation (police). We often think of state-prohibited versus state-commanded cyber attacks in similar manner. Terrorism and cyber challenge this fundamental feature. The state-crime nexus in cyber is much broader than typically conceived, with a wide gray area of direct and indirect government involvement at different levels. Jay Healey (2012) has introduced a valuable model for quantifying state involvement ranking from state-prohibited to state-sponsored, and from state-coordinated to state-integrated. It shows how governments can be involved in many ways and degrees, from actively fighting third party attacks to conducting attacks using integrated third-party proxies and state cyber forces.[4]

While there has been significant breakthrough on attribution technologies, it is the consequence of attribution that presents an even greater challenge. Attribution, hence, affects deterrence in two ways: as a technical challenge (whether or not the perpetrator can be unequivocally identified), and as a policy challenge (how you react once the perpetrator has been identified, including what constitutes appropriate retaliation). With cybered conflict short of universal conclusive attribution, the basic terms of retaliation and deterrence of the Cold War – one side strikes big and the other side retaliates bigger – are no longer valid.

In the MENA region, the lack of mature cyber capabilities prevents effective deterrence. All sides lack mature capability to identify attacks, to attribute an attack to a specific actor, and to appropriately respond with cyber operations, defensively or offensively. If attribution is always imperfect, operational and organisational maturity allows working effectively in such circumstances, and MENA governments lack this maturity. Their lack of mature capacities including in attribution, set in a highly conflictive regional environment, also means that MENA rivals are more likely to lash out against one another, especially as their lack of certainty over who attacked them makes them an easy prey for false flag operations.

The US-led Stuxnet attack on Iranian systems, first discovered in 2010, illustrates some of the deterrence challenges presented by cyber operations in the MENA region. The most immediate purpose of the operation was to retard the development of Iranian nuclear capability. Two other major purposes, however, were geared at deterrence. Threatened by Iranian nuclear ambitions, Israel was on the verge of a preventive strike on Iran when Stuxnet helped show the Israeli government that Washington was actively doing something to slow down Iran's nuclear drive. At the same time, the operation showed the Iranians that they were deeply penetrated in ways they would have never imagined, and if they proceeded with the nuclear programme, they would be hit hard. In addition, the attack implicitly suggested the degree of US readiness which, if prepared to go such lengths in the cyber domain, could go way beyond in the physical domain.

For the United States, the world's most capable military and cyber power, the Stuxnet, or Olympic Games operation[5], was an effective deterrence tool. Although resulting in only limited physical damage and not leading to a significant delay in Iranian nuclear ambitions, the attack has had an important cognitive and deterrence

[4] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," in *Cyber Statecraft Initiative* (Washington, DC: Atlantic Council of the United States, 2012).

[5] Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

effect in Israel and Iran, respectively. For Iran, retaliatory acts on US targets are likely to have contributed to an international pariah image that has ultimately driven Tehran into international isolation. At the same time, however, the Stuxnet case also shows how cyber can undercut deterrence when operations are perceived as replacing physical attacks – at least as long as physical attacks are by default perceived worse than cyber attacks, where no worst-case scenario has yet materialized.

Cyber Capabilities in the MENA

In a polarized political environment such as in the Middle East, cyber power can appear like a convenient tool for targeted political disruption. The Qatar crisis in June 2017 provided a glimpse of how targeted cyber attacks can trigger political landslides, planting a seed of misinformation in a bed of longstanding tensions.

With the exception of Israel, national cybersecurity capabilities throughout the MENA region are rudimentary, and no country can boast significant capabilities across the three sectors – government, business, and academics. Despite significant efforts to build cyber capacities in Iran and the GCC states in recent years, most countries in the MENA region still lack the three foundational elements of national cybersecurity:

1) an independent scientific, technological and industrial infrastructure;
2) a critical infrastructure protection policy, -organization, and –capability; and
3) a cyber doctrine for defensive or offensive use.

How do we quantify cyber capabilities? Unlike in kinetics, you may be able to determine manpower and budget, but not ammunition. Alongside biological weapons, cyber power is the only offensive capability in which ammunition reproduces itself endlessly. Unlike in nuclear or other conventional arms, governments are not asked to reveal their capabilities but instead their approaches to the use of cyber weapons, their concepts and doctrines. As this approach however is reliant on voluntary information-sharing, it is unlikely to produce a reliable picture of actual capabilities.[6]

However, outsourcing and proxies can offset the lack of capabilities as states in the MENA region are adamant at collaborating with non-state actors to enhance their capabilities.[7] This has frequently been the case in non-cybered conflict, such as using non-state terrorist groups for conducting hostilities on a state's behalf. Hezbollah is a prominent example. Hezbollah simultaneously conducts global terrorism, global drug trafficking, regular military activity, communal welfare, domestic insurgency, and domestic politics including participation in the Lebanese parliament and government. Some of these are proxy activities for Iran, notably global terrorism and military support to Assad's regime in Syria.

Such a multifaceted entity is the norm rather than an exception, as throughout history mercenaries and pirates collaborated with different power brokers and rulers for various interests. Therefore, a similar potential is evident in cyber. The vast supply of products of cyber crime - login credentials, credit card data, personal documents and records - have become cheap commodities on the DarkMarkets.[8] Moreover, the tools of the trade of cyber attacks - malware, exploits, toolkits, privileged credentials - are readily available and relatively affordable. Thus, state-sponsored or politically motivated threat actors can add cyberattacks to their arsenal without developing independent capabilities. Empirical evidence for collaboration between state and crime is mounting both in the commercial cyber intelligence community and in law enforcement agencies.

[6] The 2013 UN Report UNIDIR/2013/3 The Cyber Index International Security Trends and Realities is the so far most comprehensive and reliable record of government capabilities in cyber. The report is currently being updated. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
See also Global Cybersecurity Index (GCI) 2017 of the International Telecommunication Union https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[7] See also Tim Maurer: *Cyber Mercenaries: The State, Hackers, and Powe*r. Washington, DC: Carnegie Endowment, 2018.

[8] Misha Glenny, *Darkmarket : Cyberthieves, Cybercops, and You* (New York, NY: Alfred A. Knopf, 2011).

In the MENA region, the great range of different symbiotic relations between state and non-state actors extend also to cyber operations. The indictment by the US government of Iranian hackers that worked for Iranian universities but also the Iranian Revolutionary Corps Guard (see Box 1) was prosecuted as a criminal offense. The indictment also sent a signal: we are able to identify and name you individually. Notwithstanding the original motivations of the offenders, the acts acquire political significance by allowing the IRCG to enhance its capacities.

Box 1: Iran´s Mabna Institute[9]

The Mabna Institute in Iran was founded in approximately 2013 to assist Iranian universities and scientific and research organizations in gaining access to non-Iranian scientific resources. In furtherance of its mission, the Institute employed, contracted, and affiliated itself with hackers-for-hire and other contract personnel to conduct cyber intrusions to illegally obtain access to academic data, intellectual property, email inboxes and other proprietary data. The Mabna Institute contracted both Iranian governmental and private entities to conduct hacking activities on their behalf. Specifically, the Institute has conducted a university spearphishing campaign on behalf of the IRGC, coordinating a campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund since at least 2013. The Mabna Institute thus obtained more than 31 tetrabytes of academic data and intellectual property from universities, and email accounts of employees at private sector companies, government agencies, and non-governmental organizations. The defendants conducted many of these intrusions on behalf of the Iran's Islamic Revolutionary Guard Corps (IRGC), one of several entities within the government of Iran responsible for gathering intelligence, as well as other Iranian government and university clients. In addition to stealing academic data and login credentials, the defendants also sold the stolen data through two websites. *Megapaper* sold stolen academic resources to customers within Iran, including Iran-based public universities and institutions. *Gigapaper* sold a service to customers within Iran whereby purchasing customers could use compromised university professor accounts to directly access the online library systems of particular U.S.-based and foreign universities.[10]

Outsourcing criminal cyber operations to non-state groups or individual hackers presents a legal challenge in terms of the possibilities of prosecution. However, even in the absence of convictions, prosecutions and preventive measures such as travel sanctions send a strong deterrent signal to other prospective offenders.[11]

The cyber capacities of armed non-state groups to perpetrate terrorist attacks in the region and abroad remain unclear. However, contrary to common perceptions, cyber attacks provide less value for terrorism than common wisdom holds. To achieve sustained effect with cyber attacks demands a complex integrated operation and high degree of operational expertise. It is important in this regard to distinguish between information warfare and network attacks: terrorist groups such as Al Qaeda or Daesh are rather strong on the former but regarding the latter most evidence points towards them not having the necessary capabilities for major disruption. Damage assessment is complicated in cyber attacks: unlike with kinetic attacks, the damage may not be visible or straightforward. Even with tactical success, the party suffering the damage can reliably claim that the cause was a technical malfunction, not a deliberate act. This will deprive the terrorist's achievement. Low-tech attacks such as stabbing and vehicle ramming coupled with media coverage provide terrorists with much higher cost-effectiveness. It is therefore unlikely that cyber attacks will develop into a major line of action for terrorism. However, the potential remains.

[9] See the the March 23, 2018 U.S. DoJ indictment: "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[10] www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[11] For example, UN Security Council sanctions on Al Qaeda affiliates were among the most effective tools because it prevented them from traveling beyond their home jurisdiction.

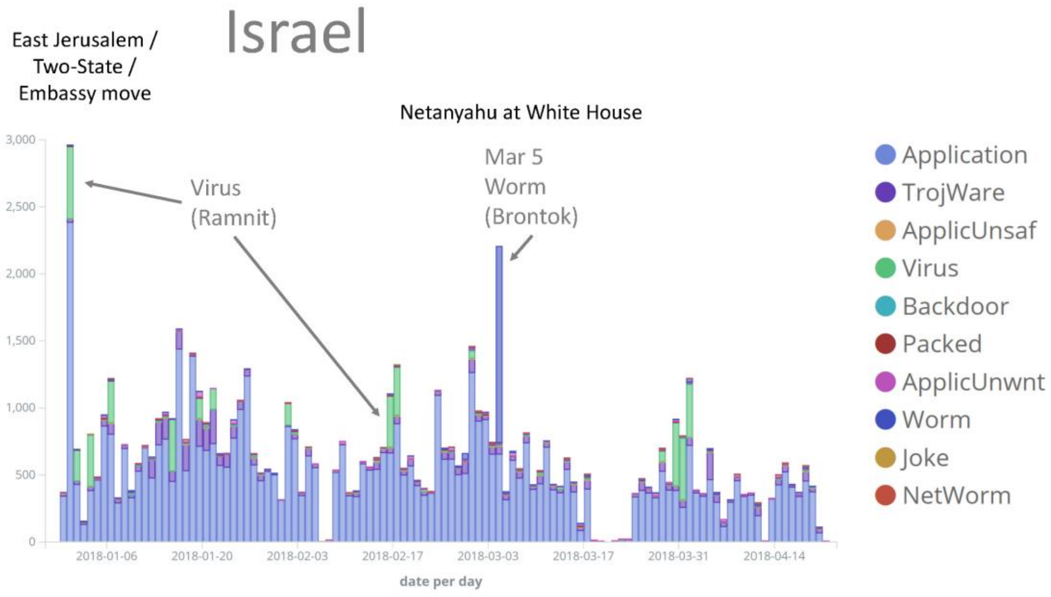
Cyber Impact on MENA Conflicts

The Middle East has experienced many firsts in cybered conflict. Stuxnet, the single most destructive cyber weapon, was uncovered in Iran’s Natanz uranium enrichment plant eight years ago. Stuxnet has been operating covertly for years at the plant and physically destroyed some 1,000 centrifuges.[12] Shamoon, a relatively unsophisticated cyber weapon, erased some 30,000 computers at Saudi Arabia's Saudi Aramco, the world's largest energy firm, in 2012. TRITON/TRISIS, the fifth industrial malware found in the wild specifically designed to jeopardize safety by disabling safety instrumentation in industrial plants, was identified in the Middle East earlier in 2018.[13] And finally, non-destructive cyber operations are more frequent and have proven to seriously destabilize geopolitical interactions. In 2017, Qatar News Agency (QNA) was hacked to publish articles on sensitive issues attributed to the country's Emir, Sheikh Tamim bin Hamad Al-Thani, leading Arab countries to launch an abrupt political and economic boycott of Qatar that holds the Gulf in a political stalemate until today.

Accumulated evidence of cyber attacks in relation to specific political events provides but a glimpse of the use of cyber tools for geopolitical purposes. Malware detections by Kenneth Geers from cybersecurity firm Comodo in select Middle Eastern countries during a given period (see charts below) shows how these network attacks conspicuously peak at moments of key political events such as political tensions, high-level visits, military deployments – although correlation and authorship may ultimately be hard to establish.

Box 2 : Malware Peaks and Political Events in Iran, Syria, Israel

Chart 1: Israel



[12] Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*.
[13] https://dragos.com/blog/trisis/TRISIS-01.pdf.
The target of the malware was the Schneider Electric's Triconex Tricon Safety Instrumented System (SIS). SISes monitor critical systems to ensure they are operating within safety thresholds; when they are not, SIS initiate emergency shutdown to prevent damage such as spill over, overheating.

Chart 2: Syria

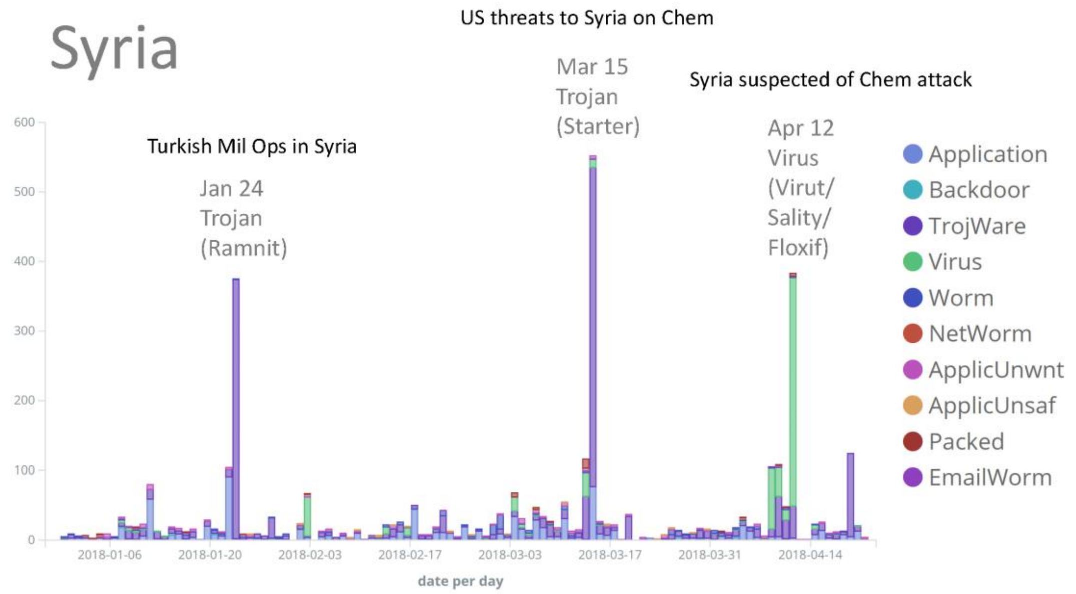
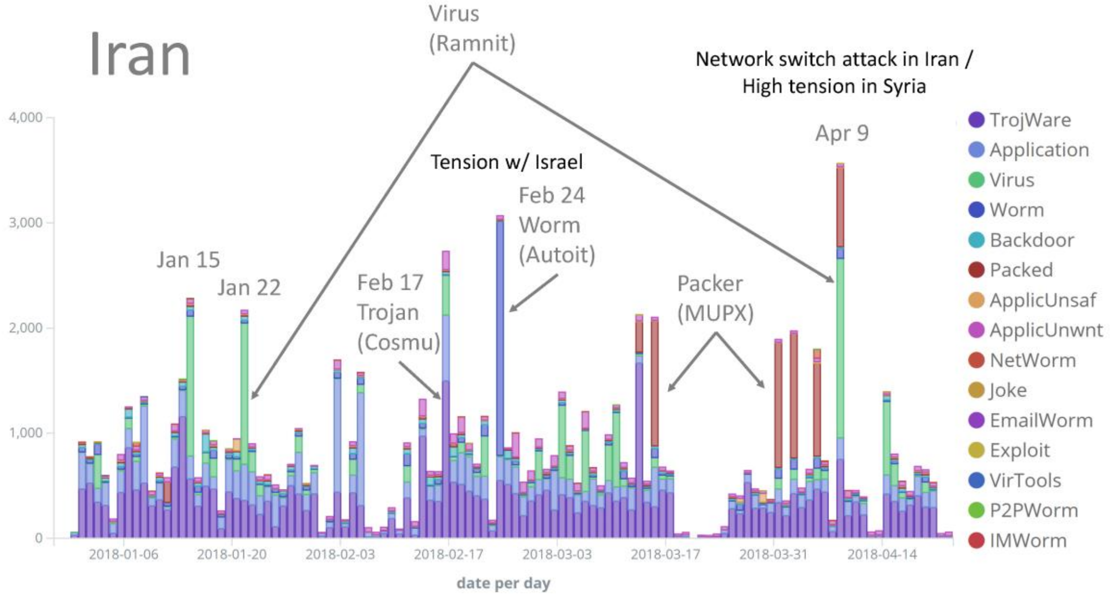


Chart 3: Iran



Russia is not only a key geopolitical actor in the Middle East but also one that has significant governmental and nongovernmental cyber capabilities. Russia has been known for its geopolitical use of cyber power, often in disruptive ways, and as experiences with Russian cyber interference in Western elections have shown, the Kremlin is not deterred by being exposed. The incorporation of cyber into the overarching military doctrine is a quite recent development in Russia. In the main two official Russian national security documents it is very clear that cyber is not only a defensive but also an offensive tool. Both documents were updated after the Ukraine crisis. The words used in these documents are not cyber but information security, or electronic warfare. Cyber security and electronic warfare are for Russia offensive tools, whereas information security is considered a defensive one.

Cyber also plays an increasing role in the *Syrian* conflict. Cyber is a good domain for regimes that cannot or will not use kinetics as their main option of warfare. Russia has been denying NATO freedom of movement in the Eastern Mediterranean, not only in military terms but also in electronic terms. It has been keen on dissimulating the scope of its role in Syria, and while kinetic assets can be seen from above, cyber assets remain largely invisible. Russia is also exploring new ways to respond to military action, as they are not interested in clashing with either the US or Israel in Syria, and cyber offers opportunities to do this with little risk of retaliation. Hizbollah's effort to step up its game in cyber has been exposed by security companies, and Hamas is also said to be developing its capabilities in cyber in both network compromising and information operations. The alliance of Iran, Syria, Hizbollah and Hamas with Russia has opened up the possibility that some Russian cyber capabilities may be transferred from Russia to Iran, and from there to Hizbollah.

Israel is a very technological state and, while this condition gives it an advantage in the cyber domain over most of its adversaries, Israel's reliance on digital technology also makes it more vulnerable to offensive cyber operations. As a result, cyber has been a key area in Israel´s broadly defined defense policy, including civilian and military sectors. Intelligence applications of cyber are numerous, advanced and critical, but naturally hidden from public sight. Israel's offensive cyber power has been displayed for at least a decade. In military operations, at least two high profile usages of cyber weapons in innovative operations are attributed to the IDF: part of Olympic Games operation this report mentioned, and Operation Orchard.[14] According to foreign sources, in Operation Orchard on 6 September 2007, the IAF bombed and destroyed a building complex in Al-Kibar, near the city of Deir ez-Zor in Eastern Syria. The building hid the construction of a graphite-cooled nuclear reactor, almost an exact copy of the Yongbyon reactor in North Korea that produces plutonium. The attack on the Syrian reactor project echoed the 1981 IAF destruction of the *Osirak* nuclear reactor in Iraq. But this time, a cyberattack allegedly was central to operational success to help overcome the Syrian air defence – the world's most dense. Allegedly, the IDF infiltrated and temporary neutralized the air defence radars and communication systems with a cyber attack, so that all aerial activity appeared to the operators as normal.[15]

Given the high dependence on advanced digital technology, Israel invests a lot in the defensive side of cyber. Since 2003, Israel's government takes responsibility to help protect civilian critical infrastructure in the nation. In 2012 a new National Cyber Bureau was established in the Prime Minister's office, following a policy review process and a national cyber strategy adopted in August 2011. Efforts to enhance national resilience against cyber threats continued: a National Cyber Security Authority was established in 2015 as a civilian cybersecurity operational agency, as was a National Cyber Event Readiness Team (CERT-IL) as Israel's national focal point for cyber security incident management. In January 2018, the Bureau and the Authority were streamlined under a new National Cyber Security Directorate.

Iran has been the main target of cyber attacks in the Middle East in both number and scope, but has also been among the main origins of MENA cyber attacks.[16] The four-decades old US-Iranian cold war, which has entered a new phase with the recent US withdrawal from the Joint Comprehensive Plan of Action (JCPOA) on Iran's nuclear facilities, has largely moved to cyberspace.[17] The leaders of the Islamic Republic are interested in cyber because, aside from stepping up their defensive capacities, it fits well with their strategic culture which emphasizes ambiguity, standoff, and the use of proxies. Unlike missiles that have a clear origin, and terrorist attacks that can be tracked down to proxies, cyber often involves a beneficial degree of ambiguity of government authorship. Iran protracts conflicts in order to achieve accumulative benefit over time. Therefore they are interested in expanding the battle time and avoiding escalation. Cyber also fits well within the narrative cultivated by the Iranian government that Iran is an emerging high-technological power, in line with their nuclear initiative. Cyber moreover allows them to do things for which they lack capacity in the physical domain. While a greater emphasis on cyber power makes sense for the Iranian regime, it also touches on some

[14] Lior Tabansky and Isaac Ben Israel, "Striking with Bits? The Idf and Cyber-Warfare," in *Cybersecurity in Israel*, Springerbriefs in Cybersecurity (Springer International Publishing, 2015).

[15] David A Fulghum, Robert Wall, and Amy Butler, "Israel Shows Electronic Prowess," *Aviation Week & Space Technology* 168 (2007).

[16] Interactive database of the publicly known state-sponsored incidents that have occurred since 2005 is available at Cyber Operations Tracker | Council on Foreign Relations https://www.cfr.org/interactive/cyber-operations

[17] Karim Sadjadpour, Collin Anderson: "Iran´s Cyber Threat: Espionage, Sabotage, and Revenge", Carnegie Endowment, 2018.

of their deepest fears, most namely domestic counterrevolution, which explains the emphasis on creating a national internet, firewalls and other control measures. The Iranian Green Movement relied a lot on social media and other web based services, so the regime sees the internet as a threat to domestic stability. At the same time, it presents unprecedented offensive possibilities. Therefore, cyber is emerging as a fourth leg of Iran´s national security strategy.[18]

Conclusion: The Middle East, a hotbed for cybered conflict

Cybered conflict is a reality worldwide. With cyber growing, Middle Eastern conflict scenarios have another layer of hybrid warfare.

The risks of destabilization and escalation are higher in MENA region than elsewhere due to a combination of five factors:

- *High Motivation*: Middle Eastern countries and factions are involved in numerous complex conflicts, both within the region and versus regional and global powers.
- *Revolutionary regional power*: a combination of ideology and realpolitik drives Iran to expand its influence in the MENA region as well as globally. Iran views cyber weapons as an affordable strategic long-range strike capability, on par with ballistic missiles.
- *Weak defenses*: most Arab countries and factions in MENA lack effective conventional armed forces and therefore struggle to achieve strategic stability. Some actors may be tempted to seek cyber weapons to gain advantages in their conflicts. In parallel, they cannot rely on conventional deterrence as their militaries also lack effective capabilities to inflict damage on most adversaries.
- *Accelerating arms races*: the GCC States have been boosting their defense expenditure for consecutive years. Arms races tend to increase the risks of hot conflicts.
- *Lack of deterrence*: most MENA states lack national cyber defense. Therefore, they are unable to detect cybered operations, cannot reliably estimate the effects, and are unable to mitigate the risks. As attribution technology drastically improved and matured in the recent years,[19] even among advanced economies few possess such mature ability, lest in the MENA. This vulnerability is clear to all actors and likely emboldens would-be attackers. Cyber attacks on the other hand can achieve a deterrent impact, as shown by the Stuxnet case.

Cybered conflict is likely to be waged with high intensity in the MENA region in the near future. The region is likely to experience unexpected consequences in terms of cascading damages, eroded deterrence, uncontrolled escalation and geopolitical fallout. Although MENA governments have limited cyber power so far, they are aware of the opportunities cyber offers and are investing heavily. This is likely to change the security equation in MENA conflicts in the coming years.

[18] See also Michael Eisenstadt: "Cyber: Iran's Weapon of Choice", Washington Institute for Middle East Policy, 29 January, 2017.

[19] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1.(2015)

Sources

Demchak, Chris C. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 121-36, 2012.

Fulghum, David A, Robert Wall, and Amy Butler. "Israel Shows Electronic Prowess." *Aviation Week & Space Technology* 168 (Nov. 26 2007): 25.

Glenny, Misha. *Darkmarket : Cyberthieves, Cybercops, and You.* [in English] New York, NY: Alfred A. Knopf, 2011.

Healey, Jason "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." In *Cyber Statecraft Initiative*. Washington, DC: Atlantic Council of the United States, 2012.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and national security,* edited by Franklin D. Kramer, Larry K. Wentz and Stuart H. Starr Washington, D.C.: National Defense University Press : Potomac Books, 2009. http://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

Lindsay, Jon R. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack." *Journal of Cybersecurity* 1, no. 1 (2015-09-01 00:00:00 2015): 53-67.

Tabansky, Lior, and Isaac Ben Israel. "Striking with Bits? The Idf and Cyber-Warfare." Chap. 9 In *Cybersecurity in Israel*. Springerbriefs in Cybersecurity, 63-69: Springer International Publishing, 2015.

Zetter, Kim. *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon.* [in English] New York: Crown, 2014.

About the authors

Kristina Kausch Kristina Kausch is a Senior Resident Fellow with the German Marshall Fund of the United States in Brussels. Her research focuses on Europe's relations with the Middle East and North Africa, political transformations in the Arab world, and broader geopolitical trends in the Middle East. Prior to joining GMF, she held positions at the Carnegie Endowment for International Peace, FRIDE, and the German development cooperation agency GIZ. She has edited three books, the latest being *Democracy and Geopolitics in the Middle East* and has published numerous articles in journals such as *International Affairs*, *Mediterranean Politics*, the *International Spectator* and *Política Exterior*.

Lior Tabansky Lior Tabansky is the Head of Research Development at the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University. His research focuses on cyber conflict strategy and operations, defense adaptation, military innovation, and comparative analysis of national strategies on cybersecurity. Prior to his current position, he served as the inaugural Cyber Warfare Research Program Associate at the Institute for National Security Studies (INSS). He also served in the Israeli Air Force and as Director of Strategy at Cyber Security Group, a Tel Aviv based cyber security business consultancy. His articles have been published among others in the *International Journal of Cyber Warfare and Terrorism* and the *Journal of Information Warfare*.

Disclaimer

The information and views set out in this article are those of the author and do not necessarily reflect the views of the KAS Regional Program Political Dialogue South Mediterranean. Reproduction is authorized provided the source is acknowledged.

Konrad
Adenauer
Stiftung

© Konrad-Adenauer-Stiftung e.V.

Programme Régional Dialogue Politique Sud Méditerranée

Le Prestige Business Center, No. F.0.1.

Rue du Lac Windermere, Les Berges du Lac

1053 Tunis

Téléphone: +216 70 029 460

Fax: +216 71 962 381

E-Mail: info.poldimed@kas.de

Web: http://www.kas.de/poldimed/en

Cover page image:
© 3109795/pixabay.com
CC0 Creative Commons