July 2019

KONRAD ADENAUER STIFTUNG

Konrad Adenauer Foundation Lebanon Office

Cybersecurity in the Middle East and North Africa

The MENA region is particularly vulnerable to cyber-attacks, at a time when cyber space is developing into a new major theater for geopolitical interaction

Valentina von Finckenstein

The number of cyber-attacks is increasing dramatically worldwide, costing the public sector and private companies globally as much as $600 billion in 2018 — about 0.8 percent of the global GDP[1]. The expanding threat landscape of cyber-attacks amounts not only to high economic losses, but endangers critical infrastructure and bears considerable political costs. While cybersecurity has received much attention in the U.S., Russia, parts of Europe and the big players in Asia over the last two decades, it has only been quite recent that the Middle East and North Africa (MENA) region started to concern itself with comprehensive debates on the issue. Most of the region's national cyber security strategies (if existing) are younger than a decade old, and governmental authorities in charge of national cyber security are being established gradually in recent years. The cyber domain as a new theatre of international interaction – a domain observing rapidly increasing popularity for new and old actors in the region - bears notable geopolitical implications for the MENA region.

This paper builds on important insights that emerged at the recent international Konrad Adenauer Foundation (KAS) MENA cyber security workshop in Beirut in April. One common denominator was evident: effective cyber security requires new ways of thinking. This ranges from approaching cyber security in a comprehensive way, to grasping its geopolitical potential and building a culture of cyber hygiene[2] for human resources and the general public.

[1] Economic Impact of Cybercrime—No Slowing Down, McAffee Report, February 2018.
[2] The term cyber hygiene refers to activities that computer system administrators and users can undertake to improve their cyber security.

Trends of the region

The vulnerability of the region

The Middle East is rapidly catching up on digitalization and expanding its information and communication technologies (ICTs) to all sectors. The digital markets of the region are expanding with an annual growth of 12%, and the number of users with access to the Internet is increasing particularly since the Arab spring 2011, with 67.2% of the MENA population having access to the Internet in 2019 (compared to the global average of 56.5 %)[3] – numbers standing in contrast with the region's preparedness. The increasing dependence on interconnectivity is touching every aspect of everyday life, including critical infrastructure. The path to digitalization, the increase of users and new technologies such as the Internet of Things (IoT) widens the field for vulnerabilities with cybercrime, cyberattacks and espionage are becoming more frequent. These forms of aggression can result in heavy economical losses and compromise intelligence integral to a nation's security.

Looking at the history and statistics of previous attacks and leaks in the region, the need for more precaution and preparedness becomes apparent. The Middle East's private sector is suffering more frequent and larger losses from cyber-attacks than the global average.[4] Poor awareness of ICT users, lack of technical capacities and a legal void all contribute to the region's attractiveness as a target. Moreover, while the attackers are increasing in numbers, "defenders" are unable keep up: governments and corporations alike struggle with a "skills gap".[5] PwC's study in 2016 found that 56% of the companies in the Middle East lost more than $500,000 due to cyber-attacks compared to the global average of 33%, and 13% lost at least three working days resulting in considerable financial losses compared to 9% globally.[6] The study clearly shows that it is not only the relative novelty of the topic that contributes to the vulnerability, but the risk appetite in the Middle East seems to differ from other regions with regard to cyber security.

The topic is still nascent in the region, and therefore often discussed one-sidedly. There is a notable tendency to approach cyber security as a mere technology issue - accordingly the states approaches to the pressing issue consist of buying technology instead of comprehensive problem solving. The private sector in the Middle East invested heavily in cybersecurity in the year 2018, a trend that will continue in 2019 with an expected spending of 1.9 Billion USD.[7] Companies in the Middle East find themselves in the global top ten in terms of investment in cyber security technology, but in the bottom 50 for cyber security education and training.[8] A technological fix, however, may create an illusion of security: the human factor, that is, the behavior of employees and users, is the root cause of successful cyber-attacks and therefore essential to address when it comes to protecting assets. MENA countries should also pay attention when buying foreign technologies. Actors often do not fully comprehend the systems and products that they acquire from leading nations in the field such as China, US, Israel and Russia, and are therefore creating new vulnerabilities with these acquisitions. The recourse to BOT systems (build-operate-transfer), in particular to technologies that surpass the buyers understanding, poses the threat of acquiring products

[3] Internet usage in the Middle East: Middle East Internet Usage & Population Statistics https://www.internetworldstats.com/stats5.htm (accessed on 25.05.2019).
[4] A false sense of security? Cybersecurity in the Middle East, PwC's study, March 2016.
[5] 2019 global State of Cybersecurity survey, ISACA.
[6] A false sense of security?, PwC's study, March 2016.
[7] Sertin, Carla, MENA companies will spend $1.9bn on cybersecurity in 2019, in: Oil and Gas Middle East (14.12.2018), https://www.oilandgasmiddleeast.com/33223-mena-companies-will-spend-19bn-on-cybersecurity-in-2019
[8] A false sense of security?, PwC's study, March 2016.

that are manipulated or flawed; in other words: products could be previously trojanized by the producer and become the entry vehicle for malicious software. This applies in particular to the GCC countries which are leading consumers of digital technology and very rarely innovators.

The vulnerability of the region is impaired by another general trend: It is becoming increasingly easier to attack an industry, while harder to defend it. It is more costly to defend assets than to develop offensive cyber capabilities. This asymmetry has led to the general trend of investing in the latter. This is especially true for state entities: although some states cannot comprehensively protect their own assets, they are able to hit back. One can observe an ongoing cyber arms race between the states of the Middle East, attempting to acquire hacking weapons and cyber experts faster than their rivals. Instead of comprehensive approaches to cyber security, safety pins prevail: some MENA countries have not even established a national cyber security strategy yet, and the governments of the region are only slowly starting to establish protection polices for critical information infrastructure and cyber-security plans.

In many states, the slow progress of digitalization processes in governmental structures and critical infrastructure has proved to be an unintended advantage to security: the lack of e-government, for instance, translates into less cyber vulnerabilities for state assets given that many relevant administrative tasks are still done on paper. But the trend of digitalization is catching up fast, in particular in the Gulf States, where it constitutes an important strand of economic policy for many governments. Saudi Arabia and the United Arab Emirates (UAE) are set out to create smart cities all over the country, while Qatar is working towards an all-encompassing smart infrastructure for the FIFA World Cup in 2022. Dubai is planning to have all its government transactions on blockchain by 2020, and many other GCC countries are investing in fintech.[9] Additionally, the heavy expenditure of IoT is touching all sectors: over 50% of businesses in the region will incorporate IoT into their work flow and investment in IoT will double from 2019 to 2021 in the Middle East and North Africa.[10] Smart infrastructure provides an excellent target, not only for hostile states, but also for small scale cyber criminality.

Geopolitical dimension

Cyber capacities of key state actors and the implications for conflicts in MENA

The history of cyber-attacks reflects the importance of cyber interactions for international relations within the MENA region. One cannot dissociate cybersecurity from geopolitics; and this is especially true for the MENA region, where cybered conflict is just one of the symptoms of wider geopolitical tensions. Cyber warfare is not only an increasingly prominent aspect of the Iranian-Saudi hegemonic rivalry in the Middle East, but also of inner-Gulf tensions and Israeli confrontation with non-state actors. This is reflected by a strong correlation between geopolitically significant events in the region (i.e. the move of the U.S. embassy to East Jerusalem or new sanctions on Iran) and peaks of malware attacks.[11] In

[9] Cyber attacks: is the GCC prepared?, The Intelligence Economist Unit (03.04.2018), https://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03 (accessed online on 05.05.2018).
[10] Westdijk, Stefan; Chaturvedi, Tushar, How IoT Will Accelerate Business Growth In MENA, in: Forbes Middle East (28.03.2019), https://forbesmiddleeast.com/how-iot-will-accelerate-business-growth-in-mena (accessed online on 03.05.2019).
[11] Kausch, Kristina, Cybered conflict in the Middle East, in: KAS Mediterranean Dialogue Series 15, August 2018.

the most pressing current confrontation between Iran and the US, both sides have augmented their resort to cyber-attacks in the past months.[12]
Attacks are being carried out on a daily basis by groups with differing affiliations, which bears a serious threat to escalate an already tense geopolitical situation in the region. Some experts even go as far as to say that *"Cyber warfare is the new normal in the Middle East"*[13]. The fact that all kinds of actors can engage in cyber operations, including non-state parties, pushes the monopoly of power further away from the state. This, in turn, leads to a sovereignty gap bigger than in other realms of conflict. Scholars have argued that cyber as a new domain of conflict creates a permanent state of potential confrontation, a state that Lucas Kello coined "unpeace"[14]: instead of being either in cyber peace or open cyberwar, we see everyday aggressions in the already geopolitically unstable environment of the MENA region. While Kello is the most prominent to argue that cyber will revolutionize the ways nations interact, other scholars doubt the impact of these technological advancements on hard power and international relations.[15] Notwithstanding the current academic debate, MENA states have shown a strong willingness to invest in both cyber security and offensive capacities in recent years.

Israel is dominating the front lines of cyber capacities, followed by its adversary Iran. The GCC states are making up ground quickly, albeit Saudi Arabia continues to have a disadvantage with regards to preparedness.[16] For the leading cyber power Israel, and particularly for the present administration, the development of cyber capabilities is one of the state's highest national security priorities.[17] The government has taken an active role in pushing the industry along. In 2011, when the National Cyber Bureau was established, its mandate included the *"vision of placing Israel among the top five countries leading in the field within a relatively short number of years."*[18] The Israeli government's cybersecurity institution, the National Cyber Directorate (a merger of the former National Cyber Bureau and the National Cyber Authority), reached a budget of $500 million in 2018. The country accounts now for the second-largest number of cybersecurity deals globally after the U.S.[19] Israel fostered a strong culture of cybersecurity with their military conscription and a highly specialised cyber-intelligence operation within the military, the Unit 8200. Furthermore, Israel is pushing an entrepreneurial approach, supporting a wide range of research including disruptive innovations and providing a fertile ground for cyber start-ups. In comparison to other Middle Eastern countries, Israel shows by far the most holistic approach when it comes to cyber security.

For Iran, cyber represents a weapon with many advantages, allowing it to strike in arenas where it physically would not be able to succeed. Iran started to show its capacities as early as 2000, when hacker groups with an evident relation to the Islamic Republic attacked networks of individuals, organisations and governments that were alleged to be hostile to Iran. The most prominent group linked to this collective that continues operating is the

[12] Barnes, Julian E., Gibbons-Neff, Thomas, U.S. Carried Out Cyberattacks on Iran - The New York Times, 22.06.2019.
[13] Anderson, Collin, How Important Has Cyber Warfare Become to the States of the Middle East?, in: Carnegie Middle East Center: Inquiring minds (01.02.2018).
[14] Kello, Lucas, The Virtual Weapon and International Order (2017), Yale.
[15] Most prominently Valeriano, Brandon and Maness, Ryan C. with "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," (2012); Gartzke, Erik with, "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth" (2013).
[16] Cyber attacks: is the GCC prepared?, The Intelligence Economist Unit, 03.04.2018, https://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03 (accessed online online 05.05.2018).
[17] Segal, Adam, Israel as a Cyber Super Power, in: Council on Foreign Relations (27.01.2016).
[18] Background for the Establishment of the Bureau, https://www.gov.il/en/departments/about/newabout (accessed online10.06.2019)
[19] Segal, Adam, The Middle East's Quietly Rising Cyber Super Power, Defense One (27.01.2016).

"Iranian Cyber Army", which, while it is pledging loyalty to the Supreme Leader of Iran, is not officially recognized as an entity by the government.[20] At the same time, Iran equally suffers from a wide range of attacks. The "Pandora's Box" of cybered conflict in the region was opened by the infamous 2010 Stuxnet virus, one of the most destructive cyber weapons seen so far. The malware impaired the nuclear plants in Iran's Natanz uranium enrichment plant, operating for years before it was officially discovered. The virus hinted towards US and Israeli perpetration and motivated Iran to invest heavily on offensive cyber capacities. Iran responded to the Stuxnet incident by attacking the computer systems of the Bank of America starting in 2011 and progressively escalating, with further attacks on US finance institutions following in 2013 and 2014. With 32 known state-sponsored offensive cyber-attacks since 2010, Iran is at the forefront of (relatively) attributable state-sponsored attacks.[21]

The Kingdom of Saudi Arabia's (KSA) cyber security sector shows an immense growth prediction for the next years. Cybersecurity is said to be one of the fastest growing segments, expanding at a compound annual growth rate of 15.3% and reaching a market value of $5.1 billion by 2022.[22] This increase is a rather reactive move resulting from numerous, regular attacks: Saudi Arabia suffers from the highest number of cyberattacks in the Middle East.[23] The target is often Saudi critical infrastructure, in particular the energy sector. In 2012, the virus Shamoon attacked the KSA's largest oil company Aramco, projecting pictures of a burning American flag on the company's computers. The so-called "9/11 of IT" exposed an industry and nation unprepared for the nature of this offense. A version of the Shamoon virus attacked Saudi government computers in November 2016, displaying a picture of the drowned Syrian toddler Aylan Kurdi. Attacks with these symbolic images play into the complex issue of attribution in international cyber conflict. Planting false flags in malware is a common tactic and one of the reasons why establishing accurate attribution is very difficult. While both Shamoon attacks hint towards Iranian authorship, some experts suggest this attack might have been a false flag operation to derail the Joint Comprehensive Plan of Action (JCPOA)[24]. This example illustrates how precarious the problem of attribution can be as a potential catalyst for escalation within the region.

A notable example of the geopolitical consequences of cyber-attacks is the aftermath of the attack on the state-run Qatar News Agency in June 2017 which plunged the GCC into a deep diplomatic crisis. After the hacking and manipulation of the Qatar News Agency, revealing emails sent and received by the Emirati ambassador to the United States were published publically. The leaking of emails was attributed to Qatar as an act of retaliation. The diplomatic escalation quickly transcended cyberspace into economic and political subversion, with an ongoing boycott of Qatar by its fellow GCC members Saudi Arabia, UAE, and Bahrain, as well as Egypt. The incident *"provided a glimpse of how the pursuit of expansive geopolitical ambitions by means of targeted cyber-attacks can generate conflict and trigger political landslides in the glimpse of an eye."*[25]

---

[20] Lukich, Alex, The Iranian Cyber Army, Center for Strategic and International Studies (12.07.2011).
[21] Council of Foreign Relations, Cyber Operations Tracker, https://www.cfr.org/interactive/cyber-operations (accessed online 1.07.2019); While attribution remains a very complex issue in particular due to the possibility of false flag operations, CRF's tracker identifies actors by using a reliable combination of technical data, open-source information, and an understanding of the threat actor's foreign policy priorities.
[22] US-Saudi Arabian Business Council, Industry Report: Defense, Security, and Aerospace (2018).
[23] Quadri, Ahman, and Khan, Muhammad .K., Cybersecurity Challenges of the KSA: Past, Present and Future, Global Foundation for Cyber Studies and Research, White Paper January 2019.
[24] Shahidsaless, Shahi,r Why would Rouhani cyber-attack the Saudis? There's far too much at stake, in: The Middle East Eye (7 December 2016).
[25] Kausch, Kristina, Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East, Policy Brief German Marshall Fund (24.11.2017).

Another interesting incident showing the shift in the Middle Eastern geopolitical landscape is the case around Saudi Arabia's spying activities on Khashoggi's communications. A lawsuit filed by the Montreal-based Saudi dissident Omar Abdulaziz identified the Israeli software company NSO Group behind helping KSA to take over his smartphone.[26] The lawsuit is also directed against the government of Israel, which licenses all sales of NSO's spyware to foreign governments. This transfer of services reveals another facet of the growing Israeli-Gulf cooperation which is starting to take on less concealed forms.

Non-State Actors in cybered conflict

States engage in multiple ways with non-state actors in cyber space in order to advance their geopolitical goals. It is important to distinguish between the particularities of cooperation as instruments within regional conflicts, as they raise different questions on responsibility, authority and control. In his pioneering analysis of the modern day-cyber mercenaries, Tim Maurer provides a useful classification of cooperation in either "delegate," "orchestrate" or "sanction."[27] If a state delegates an attack to a proxy group, it passes on the control over to a group to be in charge of specific cyber tasks. "Orchestration", on the other hand, builds on the premise that the non-state actor and state share a common ideology and goals, and that the state supports the non-state actors in their cyber activities by financial or logistical means. The loosest form of cooperation between a non-state actor and state is "sanctioning," where the state chooses to allow or even endorse the proxies' activities by not preventing or interfering. These different approaches express themselves in differing degrees of proximity: some forms of collaboration translate into close and even formal relationships, while others are intentionally hard to define, which allows their deniability. A classification of the relation is of utmost importance when it comes to the question of adequate response and how to deal with specific cyber-attacks –even more so as the use of mercenaries by states is increasing: be it for complex cyber operations, strategic messaging, or calculated escalation.

Some cyber criminals operate without any kind of significant relationship to a state and/or without a connection to a geopolitical agenda. In general, cybercriminal sophistication is developing in the MENA region, with an underground market that is rapidly maturing. With increasing digitalization of financial transactions, rising numbers of users and access to user's data, criminals are finding new ways to line their pockets. The focus of cybercrime is growing on the expanding IoT vulnerabilities within the region.[28] For many non-state actors, the cyber domain presents new ways for achieving old ends, such as acquiring resources. The Houthis for example, an armed Islamic group rebelling against the government in the ongoing Yemeni civil war, successfully increased their revenues by engaging in large-scale crypto currency mining.[29]

However, the development of an attack with real-world impact is complex and requires capacities that not many states, let alone non-state actors, possess. State-sponsored attacks therefore present a much bigger threat than the capabilities of autonomous actors such as ISIS and al-Qaeda. Entities with limited capabilities draw back on social engineering or information engagement rather than attacks on critical infrastructure: Propaganda and

[26] Kirkpatrick, David D., Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says, in: New York Times (2.12.2018) https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html (accessed online 25.06.2019).
[27] Maurer, Tim, Cyber Mercenaries: The State, Hackers, and Power (2018).
[28] Fuentes, Mayra; Aly, Ahmed, Cash and Communication: New Trends in the Middle East and North Africa Underground, Micro Trend Study (27.11.2018).
[29] Groll, Elias, The Other War in Yemen—for Control of the Country's Internet, in: Foreign Policy (28.11. 2018) https://foreignpolicy.com/2018/11/28/the-other-war-in-yemen-for-control-of-the-countrys-internet/ (accessed online 20.05.2019).

information gathering is more prevalent because it is more feasible. In particular for ideologically driven non-state actors with dwindling physical resources and territories, strategies shift towards the online world, where movements and ideas can expand cross borders and online presence reaches a wider audience. The cyber operations of the Palestinian group Hamas, however, show that limited resources can also have an impact on high security institutions: the hackers created so called honeypots, set up fake dating and FIFA World Cup apps targeting IDF recruits in bases around the Gaza strip and managed to gather sensitive information on locations and soldier's private data.[30]

Asymmetric and proxy warfare are common military and political strategies in the geopolitical confrontations of the Middle East. These strategies perfected in the physical realm are mirrored in cyberspace. In particular state and non-state actors with a strong focus on asymmetric warfare in their strategy engaged from an early time on in cyber operations (Iran, Hamas, and Israel). Iran, a power that is very well experienced in asymmetrical warfare, makes frequent use of orchestrating operations in the cyber realm. The Islamic Republic is believed to have lent support to Cyber Hezbollah, the Syrian Electronic Army, the Yemen Cyber Army, Hamas and many other groups.[31] For states or political actors, delegating cyber-attacks to mercenaries or proxies bear many advantages: first and foremost one can deny responsibility and the costs are likely to be lower (both aspects also bear the potential of escalation). Yet unlike traditional transfers of arms or equipment to proxies that require regular supplies, the transfer of cyber resources and tools remove these technologies from state control. Exerting control over proxies in cyber warfare thus becomes harder than in the physical world.[32] Next to the complexity of attribution and the low costs, this might present an additional escalating factor.

The question of retaliation is a very sensitive one. Aside from reactive responses, can and should one defend against aggressors by offense? Hacking back can serve as a form of deterrence. Immediate retaliation, however, requires the state to attribute the attack to an actor. The lack of digital evidence in combination with the transnational character of cyber technology and activity makes attribution very complex and requires sophisticated technologies. With regard to retaliation, an incident of a Hamas cyber-attack in early 2018 deserves special attention. The group sought to hack the IDF, which had a rapid kinetic response as a result: the IDF launched an airstrike on a building in Gaza from which the hackers were allegedly working from. This reaction sets a precedent in cyber conflict and shows the potential of physical consequences of cyber conflict in the future.[33]

Protecting Critical Infrastructure

Cyber warfare in the MENA region comes in different shapes and forms and is directed against various targets. The most feared disruptive attacks are acts of cyber terrorism, disabling or gaining access to industrial systems or attacks on critical national infrastructure (CNI). Worst case scenarios of cyber warfare often envision such an attack on CNI's by a hostile government or a terrorist group - nevertheless this occurs rather rarely in proportion. As of now, not only malicious technologies present a threat to CNI cyber security, but in particular human behavior that allows leakages: employees remain the weakest link in CNI cyber security. The challenge here is often to judge whether the behavior

[30] Ahronheim, Anna, Hamas using honeypots to target Israeli soldiers on instagram, in: The Jerusalem Post (14.08.2018).
[31] Sulmeyer, Michael, Cyberspace: A Growing Domain for Iranian Disruption, Center for Strategic and International Studies (03.2017).
[32] Kausch, Cheap Havoc (2018).
[33] Groll, Elias, The Future Is Here, and It Features Hackers Getting Bombed, in: Foreign Policy (6.04.2019), https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/ (accessed online 25.05.2019).

of employees is malicious or well meaning. Relatively simple human actions can compromise sensitive data of critical infrastructure, such as sending an email to the wrong address.

In the cyber-ecosystem of CNIs, all actors are vital for protection: government, company and user. The complexity of technology systems and their all-encompassing nature do not allow a single actor to be blamed. Responsibility is an important, albeit very complex question when it comes to CNI. In many states where critical infrastructure systems such as health, finance and transport have been privatized, the extent to which the state can outsource authority and responsibility for national security becomes a critical issue. One of the core responsibilities of a state is providing national security by protecting CNI. Passing on this responsibility to the private sector raises many sensitive and urgent questions.[34] In light of the current trend in several MENA countries to liberalize sectors such as telecommunication, transport and energy, this question needs to be reflected very well.

One of the industries that faces a particularly strong risk is the financial sector, as almost all transactions nowadays rely on digital processes. The sector has suffered many losses by cyber criminals and state-sponsored attacks alike, targeting small entities, but also major banks. In 2012 and 2013 alone, RAK Bank (UAE) and BMI (Oman) suffered attacks which caused a loss of $ 45 million. States such as Lebanon, which are heavily reliant on their financial sector, are particularly vulnerable.

Yet the digitalization of critical infrastructure creates vulnerabilities that seem to be nowhere as pressing as in the MENA's energy sector. It has been traditionally the motor of growth in many of the Gulf economies. With the states' heavy reliance on these incomes, rigorous securitization of this infrastructure is vital. The sector, however, is still unprepared for today's challenges. According to a study conducted by Siemens, the industry was the target of 50% of all cyber-attacks carried out in 2018.[35]

The industry is facing in particular rising operational technology (OT) cyber risks: 30% of attacks are targeting OT,[36] as "convergence of IT and OT has become a key opportunity for attackers to infiltrate an organization’s critical infrastructure, disrupting physical devices or operational processes"[37]. Attacks in the industry are very regular, thus risk management is essential. The extended infrastructures of oil and gas in remote locations present an additional challenge once physical harm results from cyber-attacks.

Among the most famous incidents is the above mentioned malware Shamoon that was used to attack Aramco in August 2012. The company was forced to shut down their network and destroy 35,000 computers. The same virus was found later in Qatar's GasRas.[38] Disrupting operations of the MENA oil companies such as Aramco, the world’s largest oil company, would not only have disastrous consequences for the flow of oil, gas or electricity, and the KSA economy as a whole: it would bear implications for the world markets as well. Here, as also in many other sectors, not only the cyber security budgets and investment in new technology needs to increase. It is essential that awareness and cyber hygiene increases in order to secure the operating environments,.

[34] Carr, Madeline, Public–private partnerships in national cyber-security strategies, in: International Affairs Chatham House 92: 1 (2016).
[35] Siemens report 2018: Assessing the Cyber Readiness of the Middle East's Oil and Gas Sector, http://www.middleeast.siemens.com/me/en/news_events/news/news_2018/siemens-report-mideasts-oil-and-gas-sector-needs-readiness-boost-as-cyber-risk-grows.htm (accessed online 24.05.2019).
[36] Ibd.
[37] Ibd.
[38] Fineren, Daniel, Qatar's Rasgas hit by computer virus, in: Reuters (30.08.2012), https://in.reuters.com/article/qatar-rasgas/update-1-qatars-rasgas-hit-by-computer-virus-idINL6E8JUD1K20120830 (Accessed online 30.05.2019).

Legal framework and civil rights

The exponential growth of digital interconnectivity is accompanied by a lack of domestic and global governance, conventions and cooperation. Without harmonizing laws regionally, safe havens for cyber criminality are hard to combat. Few countries in the Middle East possess concrete cyberlaws that are successfully enforced. Effective online law enforcement requires the smart use of innovative technologies, but it also presupposes lawmaking in form of precise and comprehensive laws that carry provisions for procedure as well as criminalisation. Where domestic cyber laws are enacted in the MENA region, they often assume vague shapes and leave room for grey zones and misinterpretation.[39]

Legal frameworks of cyber policy cannot be separated from the political dimension. The EU's efforts to ban Huawei to secure its 5G network, for example, shows clearly the layering of geopolitical interests and cyber regulations. An important issue with cyber regulation in the Middle East is that it can be easily used as a pretext for states to implement laws in order to clamp down on dissidents, monitor its citizens and censor unwanted content.[40] The focus of the national cyber laws that do exist in the region often lies on criminalizing speech and online activities, in particular with regard to criticism towards the government, religious leaders, but also online communities which organize protests.[41] Cyber laws frequently clash with civil rights and privacy. The essential catalyst for this increasing tension was the Arab Spring: During the upheavals in the Arab world, social media represented a new political platform for citizens to express their grievances in a way they were denied in the physical world. As demonstrations usually took place on the streets, the virtual space was not a security concern for governments. In this sense, the Arab spring presented the tipping point in MENA media development. To keep the population in check, many governments resorted to restricting online platforms or using new technologies as surveillance tools.

Iran is investing heavily in offensive cyber capabilities and has particularly used its cyber tools to spy on critics of the government and to deny access to information. In the aftermath of the Green Revolution in 2009, Iran made sure to advance its cyber capacities to bring the upheavals under control. This translated into increasing surveillance and the constraining of digital freedom and civil rights. In attempting to confine the possibilities of an unregulated Internet, the Islamic Republic is regularly shutting down access to some of the country's most popular social media sites, and resorts to Internet slowdowns in order to frustrate users.[42] In 2018, Egypt enforced a law that endorses Internet Service Provider (ISP) surveillance and gives the government the authority to censor and shut down content that "threatens national security" - an expression that leaves room for broad interpretation.[43] The GCC countries - where free expression is traditionally more restricted[44] - have enacted or updated their cybercrime laws from 2011 onwards. These cyber laws focus on limiting freedom of expression, seeking to get a stronger grip on social media. Meanwhile they lack mechanisms to tackle actual cybercrime.[45]

---

[39] Hakme, Joyce, Cybercrime Legislation in the GCC Countries Fit for Purpose?, Chatham House Publication (4.07.2018).
[40] Ibd.
[41] Ibd.
[42] Eisenstadt, Michael, Iran's Lengthening Cyber Shadow, Washington Institute for Near East Policy Research Notes 34 (July 2016).
[43] Samir, Mohamed, Al-Sisi ratifies cybercrime law regulating web content, ISP surveillance, in: Daily News Egypt (18.08.2018), https://www.dailynewsegypt.com/2018/08/18/al-sisi-ratifies-cybercrime-law-regulating-web-content-isp-surveillance/, (accessed online 30.05.2019).
[44] In the press and internet freedom ratings of Freedom House all but Kuwait are rated "not free," (Kuwait is rated as "partly free") and no Arab state is considered "free": Freedom in the World 2018, Freedom House, 2018, https://freedomhouse.org/report/freedom-world/freedom-world-2018 (accessed online 30.06.2019).
[45] Hakme, Joyce, Cybercrime Legislation in the GCC (2018).

When talking about media and information, the disinformation resilience of governments and the manipulation of information online are rising concerns for governments. While these challenges do not necessarily result in physical damage, they can be detrimental to civil-government relations. The damage of fake news can result in a loss of trust in the state system and destroy the trust in public debate. Fake news is especially problematic in democratic societies, as the informational environment is key for opinion forming and election behavior. Democracies are less likely to survive when citizens are poorly informed.[46]

However, fake news does not play the same role in the MENA region as they do in the Western world - not least because the forms of government differ widely from each other. In addition, the media scene in the MENA region is in most cases state, semi-state or party controlled. Calling for regulating fake news and hate speech in these structures could come at the expense of civil liberties. The bias for regulating fake news should impede governments from taking this action.

While foreign interference in elections is a major topic in the West, this kind of cyber meddling is not yet relevant in MENA. Here again, lagging behind in digitalization produces benefits: as the election processes are still mostly executed on paper, entry points for hackers are scarce.

Recommendations

- Security hygiene in MENA is key: There is not enough awareness in the public domain. Users need to understand the devices and systems they are using. Countries in the MENA must continually raise their citizens' awareness regarding cybersecurity and this should be built from a very young age.

- Private companies in the MENA region must be incentivized by the state to have a holistic strategy for cyber security. To guarantee compliance with existing cyber laws, a carrot and stick strategy could prove to be useful: harder legal consequences for breaches on the one hand (including making the Chief Information Security Officers CISOs of companies more accountable), and setting financial incentives such as tax returns on the other hand to encourage cyber hygiene.

- The training of human capital is one of the most important steps to make companies, governments and critical infrastructure more resilient. The technocentric approach of many MENA countries, which try to tackle security risks by acquiring technology, falls short: smart budget allocation and a holistic view that reflects the human factor is essential. Actors should be encouraged to invest in people rather than placing all hopes on the redemption by cybersecurity technologies.

- Developing a common language is important to connect expertise with relevant policy makers: the cyber-specific language has to be translated in order to make the topic accessible for those who shape the policies.

- From a reactive towards a proactive approach: There is a lack of investment in disruptive innovation in the Middle East, but also in Europe. Analysing worst case scenarios for

[46] Hollyer, James, et al., Information, Democracy and Autocracy: Economic Transparency and Political (In)Stability (2014), pp. 413-434.

cyber warfare and anticipating the threats of tomorrow is essential in light of the enormous speed and scale of new technological developments. AI powered attacks are likely to be the next, great challenge for cyber defense - governments and companies alike need to be prepared.

- The creation and support of excellence centers, such as NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE), and exchange of expertise between these hubs is important for the region's preparedness.

- Cooperation: The main challenge is bringing together key stakeholders. This includes interstate, public-private and provider-user cooperation. More initiatives are needed. In particular effective private-public partnership needs to intensify. A relationship based on mutual trust can better keep up with necessities and makes a rapid exchange of information possible. Additionally, more measures have to be taken for the cooperation of different agencies concerned with cyber security.

- It is necessary to foster coordination among each of the country's sectors toward shared cyber goals. Competences and capacities in the field of attribution and deterrence must be developed and expanded across borders.

- MENA countries must develop solid and sustainable National Digital Security Strategies, including the set-up of National Computer Emergency Response Teams (CERTs).

- In order to fill the legal void, MENA countries could orient themselves towards several existing conventions. Among these is the Budapest Convention of Cybercrime, which aims to address cybercrime by harmonizing national laws and increase international cooperation. Composed by the Council of Europe in 2011, this convention was the first of its kind. Another step forward could be to encourage MENA countries to sign the Paris Call for Trust & Safety in Cyberspace. Currently only four countries from the region have signed it, namely Lebanon, Morocco, Qatar and the UAE. Moreover, the region would benefit extensively from following the reglementation of the GDPR, the EU law on data protection and privacy for EU citizens. This would be an effective incentive for entities which handle data of users to maintain a higher standard of cyber hygiene. These conventions, however, do not replace the creation of a necessary legal framework tailored to the MENA region, as the environment differs from its Western counterparts: the relation between government and private sector, prevalent critical infrastructure, cultural factors, domestic regulations, and last but not least – geopolitics - all have to be taken into account. At the same time, state-level regulations are not enough, and might create a false sense of consumer confidence: regulation is necessary, but not sufficient. The formalization of intention needs to be accompanied by the will to install governance.

- One cannot dissociate cybersecurity from freedom of expression and public liberties in each country of the MENA region. When pushing for stronger legal reglementation of cyber space, policy makers, civil society and the private sector should be very attentive to possible restriction of civil rights.

- Concerning fake news, the governments should not over-regulate the access to information for users. Bottom-up approaches are more likely to be reconcilable with civil liberties. Civil society should be included in the process, particularly for the sake of social compatibility and stability. Moreover, it is important to support media awareness and

media literacy from a young age, educate citizens and support local and independent media.

Konrad-Adenauer-Stiftung e. V.

Valentina von Finckenstein
Research Associate
valentina.vonfinckenstein@kas.de

KAS Lebanon Office
www.kas.de/lebanon