OPEN PUBLICATIONS

Cybersecurity in the Middle East and North Africa

Volume 10, Number 3, 2025

ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

DISCLAIMER:

Let us know your thoughts on "Cybersecurity in the Middle East and North Africa" by emailing us at:
editor@openpublications.org

www.openpublications.org

CREDITS

CONTRIBUTING AUTHORS

Professor Fabrizio Enrico Erminio Baiardi,
Department of Computer Science,
University of Pisa

OPEN CAPABILITY LEADER

Col Stefan Lindelauf

OPEN LEAD EDITOR

Mr Jeffrey Reynolds

OPEN OPERATIONS MANAGER

LTC Alexios Antonopoulos

ACTION OFFICER

Mr Francisco Saez, NSD S HUB

OPEN EDITORIAL REVIEW BOARD

LTC Tor-Erik Hanssen
CDR Silvio Amizic
CDR Alan Cummings
LTC Claus Slembeck
LTC Anders Wedin
LTC Mithat Almaz
LTC Gabor Farkas
Ms Klodiana Thartori
Mr Helmar Storm
Mr Theodore Rubsamen
Mr Christopher Hall

TECHNICAL EDITOR

Dr. Maureen Archer

ART DESIGNER

PO1 Emilia Hilliard

CONTENTS

CYBERSECURITY IN THE MIDDLE EAST AND NORTH AFRICA

FABRIZIO BAIARDI
DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF PISA

ABSTRACT

The Middle East and North Africa region (MENA) is strategically important as it lies at the crossroads of Africa, Asia and Europe. This work analyses the current status of cybersecurity in MENA and its expected evolution. Accordingly, the work is organized into two parts. The first discusses the global cybersecurity status of the MENA region and then focuses on three scenarios: North Africa, Israel and the Gulf region. For each scenario, we point out the trends of cyber intrusions to anticipate possible evolutions. The main focuses of this part are the Hamas and Israel conflict, the attacks on the financial sector, and the production and transport of oil and gas in the Gulf. We also discuss changes in the conflict between Israel and Hamas before and after the October 7th attack and the role of Iran.

The second part of this work is split into three sections. The first reviews cybercrime and data protection legislation in the MENA states. The second evaluates the capabilities and intent of the various states in MENA. This part discusses the current legislation of the states and analyses some rankings of the states to estimate their ability to defend their infrastructures and the resulting cyber resilience. The last section discusses strategies to improve the overall cybersecurity status. It considers three critical issues that affect these strategies: supply chain attacks, ransomware, and spyware. We also discuss the role of private-public cooperation and cyber security start-ups in Israel. Lastly, we suggest the adoption of a proactive approach, based largely on what would be considered valid worldwide.

Keywords: *supply chain attack, ransomware ecosystem, spyware, industrial control system, wiper*

EXECUTIVE SUMMARY

The current cybersecurity status in North Africa and the Middle East (MENA) is analysed herein by researching three distinct scenarios (North Africa, Israel, the Gulf region). Each scenario is characterized by proper cybersecurity aspects concerning threat agents, intrusions and impacts. Firstly, the North Africa region faces traditional cybercrime with threat agents organized in gangs, where the main goal is economic benefit. The second relates to the ongoing conflict between Israel and Hamas. Here intrusions are focused on the collection of intelligence information to plan military action and anticipate adversaries' actions. The distinguishing features of the third are intrusions against the industrial control systems that manage oil and gas extraction and distribution together with ransomware intrusions that mostly target financial institutions.

The work discusses the cybercrime and privacy legislation of nations in the MENA region by reviewing the various legislation, the protection of personal data and differences with respect to the usual European approach. The paper describes alternative ranking strategies that have been proposed to estimate the cyber offensive and defensive capabilities of the various States to protect their infrastructures and respond to attacks. A joint analysis of these aspects is useful to estimate the overall cyber resilience of the region. A detailed evaluation of the indicators that have been used to define the ranking can point out important differences between states in MENA. This part of the work identifies how the cybersecurity, robustness and resilience of each state results from a compromise between two competing capabilities: increasing the robustness of the Information and Communication Technology (ICT) and Operational Technology (OT) infrastructures of the State and successfully dismantling the attack infrastructures of adversaries. A separate evaluation of each of these capabilities conveys useful information to assess strengths and weaknesses of a State.

Lastly, we formulate some suggestions on how NATO can support an increase in the overall cyber resilience in MENA. These suggestions include improved public/private cooperation to improve defence against hybrid and state-sponsored threats. The problem posed by the wide adoption of spyware is also examined. More in general, a suggestion is made that NATO could sponsor and support a more proactive approach to cybersecurity. The expected benefits of this approach are critical both for countering terrorist organizations in the region and for the importance of oil and gas supplies for several NATO nations. Examples and lessons learned, including in other regions besides MENA, confirm the advantages of improving the cyber resilience of such a critical region as MENA.

This work relies on open and publicly available sources as of the end of July 2024. This places a clear caveat on its findings because it is impossible to arrive at a complete and confident picture of cyber operations when most data on these operations are classified.

INTRODUCTION

This work describes the current cybersecurity status of MENA and is organized into two parts. Part I discusses the global cybersecurity status of MENA by researching three distinct scenarios (North Africa, Israel and the Gulf region), which differ in the most important cybersecurity aspects: threat agents, intrusions, and impacts. The North Africa region goes from Egypt to Morocco and Mauritania. This is an area marked by traditional cybercrime, where most threat agents are organized in gangs with economic benefits as their main goal. The second covers Israel and the ongoing conflict between Israel and Hamas. In this scenario, which includes Jordan, attackers aim to collect intelligence information to plan military action and defeat the actions of the opponent. The third area concerns Saudi Arabia, the Emirates and Iran. This scenario is characterized by two important kinds of intrusions: those into industrial control systems (ICSs) that manage oil and gas extraction and distribution [18], and intrusions that include ransomware against financial institutions [19,41].

Part II evaluates the capabilities and intent of the various states and focuses on three topics. The first concerns cybercrime and privacy legislation. The various legislation is reviewed and the privacy of personal data in the region is discussed. The differences concerning the European approach to the protection of personal data are also pointed out. The analysis includes alternative rankings of the states to estimate their cyber offensive and defensive capabilities to protect their infrastructures and respond to attacks. A joint analysis of these aspects defines the overall cyber resilience of the region. Next, the intent and capabilities of states within the region are analysed. An index is used that is believed to be capable of forecasting the robustness and resilience of the ICT infrastructures of the various states and of the ICSs connected to these infrastructures. A detailed evaluation of these indicators points out important differences between states in MENA.

The last section of Part II considers examples and lessons learned, including in other regions besides MENA, to exploit previous experiences to the fullest. The section also formulates five recommendations for NATO that concerns

1. the public disclosure of vulnerabilities,

2. the dismantling of attack infrastructures,

3. the definition of standards and best practices for equipment acquisition, management and dismissal,

4. favouring robustness with respect to resilience,

5. a strong cooperation with the public sector.

We believe they are fundamental to opposing the terrorist organizations in the region and for the critical role of oil and gas supply for several NATO nations. The impact of a secure supply chain and spyware on the overall cybersecurity of the region is included, ending in evidencing the importance of a proactive approach to cybersecurity. An organization like NATO could play a fundamental role in enhancing cooperation in the area so that regional organizations and nations can enhance their resilience. The clear benefit for NATO is better resilience in a critical region because it is well known that resilience depends upon the weakest link. Hence, it is hard to overestimate the importance of increasing the resilience of all nations in the area.

A fil rouge, or unifying concept, of this work is that the attitude of a state towards cybersecurity,

robustness and resilience results from each state's compromise between two competing capabilities, where a capability includes know-how, tools and abilities. The first capability of interest is to increase the robustness of the ICT/OT infrastructures of the state that result from the interconnection of ICT infrastructures with operational technology (OT) that describes the technology of ICSs. The second capability is to successfully attack adversaries' infrastructures, including their attack infrastructures. As discussed more deeply in Part II, Section 2, these are the critical capabilities to evaluate how a state can resist intrusions and protect its own critical ICT/OT infrastructures, as well as to dismantle the network infrastructures that can be used against the state. Other important capabilities of a state, such as collecting information on adversaries, can be deduced from them.

PART 1

1. Baseline of the current cyber domain in MENA countries.

Before discussing each of the three scenarios previously introduced, some global data on the overall cybersecurity scenario in Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) countries is presented.

Very little data and statistics are public on attacks in MENA [6, 19, 20, 24, 25, 40, 51] and even less for single states. We only know that in 2023 about 1% of all attacks targeted organizations in North Africa and 5% in the Middle East [15]. Another contribution for estimating the level of "cybercriminality" present within each country in MENA is [8] an expert survey where participants were asked to consider five major categories of cybercrime, to nominate the countries that they considered to be the most significant sources of attacks in each category, and then to rank each nominated country according to the impact, professionalism and technical skill of its offenders. This resulted in the World Cybercrime Index, a global metric of cybercriminals in a country. This index also offers valuable insights into the dimension of cybercrime local to a nation. Russia is at the top with a score of 58.39 while Fig. 1 shows the position of nations in MENA.

To improve the evaluation of MENA's cybersecurity status, the information for sale on dark web markets in MENA states [21, 33] can be used. According to experts, the status of markets in the dark web related to MENA is very similar to the one in France, because seeing and buying most of the physical and virtual objects on sale requires both registration and authentication. Registration implies a vetting process, a joining fee paid in Bitcoin, and even a language barrier because most underground sites are in Arabic, even if several members also post in English, and occasionally, in French. One of the services offered in the dark markets is a Distributed Denial of Service attack. This attack is employed by threat actors in the regions to support their political activities.

A more updated description of the information for sale on the dark web comes from "underground clouds of logs" (UCLs) [22]. This is an emerging means of buying and selling data in forums on the dark web. The information in a log is the output of an information stealer, a malware that collects credentials saved in browsers, such as bank card details, crypto wallet information, cookies, and browsing history, and then sends all this data to the malware operator that then sells it on the dark web. Information stealers have emerged as a major source of compromised personal data due to their simplicity and effectiveness. After being

Position	Nation	Score
11	Iran	4.78
16	Israel	2.51
24	UAE	1.55
48	Morocco	0.45
69	Tunisia	0.22
94	Syria	0.09
97	Egypt	0.08

Fig. 1 Ranking of the Cybercriminal Ecosystem in Some Countries

installed on a machine, a stealer generates a log with the information it has collected and then it sends this log to the private cloud-based platforms of the attackers. This platform hosts the cloud of logs that are made available to the interested party through data analysis and extraction tools. Fig. 2 shows the number of available logs on the dark market for some states in MENA.

Nation	Score
Turkey	58,092
Egypt	56,222
GCC	27,226
Algeria	26,805
Morocco	24,203
Iraq	11,254
Tunisia	9,619

Fig. 2. Number of Logs on Sale for Some Countries

The last perspective is related to cryptocurrency. According to Chainalysis [10, 33], in 2023 MENA had the sixth largest crypto economy in the world with an estimated $389.8 billion in value received between July 2022 and June 2023. This represents nearly 7.2% of global transaction volume during the period studied. MENA is also home to two of the top 30 countries in the 2023 index: Morocco (20), and Iran (28). UAE sees a much higher share of crypto activity taking place than its regional neighbours, apart from Israel.

1.1 Main risks and challenges to the Cyber domain: North Africa

INTERPOL reported on Africa in 2022 and 2023 [25,26], identifying some prominent trends:

a) Campaigns to compromise business emails are the most prevalent cybercrime.

b) Phishing is a growing concern due to the rapid adoption of digital technologies.

c) Online scams are becoming more popular as the internet is becoming widely available.

d) The number of ransomware intrusions has been increasing rapidly.

e) Banking Trojans and stealers pose an emerging and imminent threat to online shoppers.

f) Some gangs experiment with their latest ransomware on businesses in Africa, before targeting richer countries with more sophisticated security methods.

The number of cybercrime gang intrusions continues to rise across the African continent. The average number of weekly cyberattacks per organization increased by 23% year-on-year in 2023, which is the highest average in the world.

Several non-government organizations (NGOs) claim most nations in this area have used spyware to monitor opposition. The most well-known spyware is Pegasus [14] which was designed by an Israeli NSO Group to access sensitive information on the devices of terrorists, criminals and other people identified as potential threats. Pegasus spyware can infect an iPhone or Android device without any action from the victim, and it can track phone calls, location, text messages and emails. Researchers discovered that thousands of people may have been monitored using Pegasus including dissidents but even members of royal families. Nations involved include Egypt, Tunisia and Morocco. One of the most recent events occurred in April 2024[1] when a new mobile malware masquerading as a news app was spotted targeting human rights activists associated with the Sahrawi Arab Democratic Republic, SADR. This is a malicious Android mobile app that pretends to be a variant of the Sahara Press Service app, run by a media agency associated with SADR. The custom-built application was distributed through spear phishing emails to human rights activists in Morocco and SADR, also known as Western Sahara.

1.2 Main risks and challenges to the Cyber domain: Israel, Hamas and Iran

This scenario considers the cyber conflict between Israel, Hamas and Iran, and it has completely changed since the 7 October 2023 attack. This is a scenario where the ability to attack and penetrate the adversary infrastructure dominates.

Before 07 October, Hamas cyber wings routinely resorted to disruptive operations to break the cyber blockade by targeting Israeli cyberspace,

[1] *https://therecord.media/android-mobile-spyware-western-sahara*

on both its military and civilian nodes [12, 48]. The offensive tactics of Hamas include intrusions to gather intelligence, as well as disruptive ones that intensified during Israeli raids and have been a constant feature in the last ten years to support attack planning. Hamas used unsophisticated coding but advanced social hacking techniques that specifically targeted military and government personnel with highly designed baits and highly tailored content. In 2023 the Google Threat Analysis Group, TAG, discovered and disrupted Hamas operations to distribute Android spyware with standard mobile spyware functionality, including the permissions to read contacts and SMS (Short Message Service) data. It can also send SMS messages phishing for additional targets. More recently, some Hamas-linked actors have shown advanced capabilities, including elaborate social engineering and custom malware developed for Windows, Mac and Linux.

In the six months before the 07 October attack, Iran accounted for about 80% of all government-backed phishing activity targeting users based in Israel. Iran-sponsored threat actors accounted for most of this activity, with targets including national and municipal governments, diplomatic organizations, academia, think tanks, NGOs, media, technology companies, aerospace and defence, and the shipping sector.

In the weeks leading up to 07 October, Hamas-linked actors launched multiple campaigns targeting users and organizations based in Palestine and those in the Fatah-led government. These campaigns point out that Hamas focused on collecting intelligence about internal Palestinian affairs, even weeks before launching a major attack on Israel.

According to public information, Hamas intentionally did not use cyber operations to tactically support the 07 October attack. This is in stark contrast to Ukraine with a large increase in Russian cyber threat activity targeting Kyiv in the lead-up to the invasion.

After 07 October, intrusions against Israeli organizations have more than doubled.[2] There has been a focused effort to undercut support for the war among both the Israeli public and the broader global populace, including hack-and-leak and information operations to demoralize Israeli citizens, erode their trust in national organizations, and cast Israel's actions in a negative light. As in the past, Iran-sponsored threat actors have shown a capability and willingness to carry out destructive and disruptive intrusions against targets spanning a range of regions and sectors, including those in Israel. In the weeks following 07 October, destructive cyberattacks have increased, including

[2] *https://therecord.media/android-mobile-spyware-western-sahara*

the deployment of wiper malware targeting the Israeli government, financial institutions, tech companies, and defence contractors.[3]

Hezbollah, an Iranian proxy, also conducted cyber operations targeting Israel immediately after 07 October.

1.3. Main risks and challenges to the Cyber domain: The Gulf Region

The third scenario includes Iran, Saudi Arabia, and all the states of the Gulf Region. The two main actors are Iran and Saudi Arabia. Even in this scenario, intrusions into adversary infrastructures dominate. Here intrusions target ICSs, mainly those related to oil and gas extraction and distribution, where Iran is the main actor [2, 11, 18]. Further intrusions we consider are those related to ransomware [19, 34, 41]. Even several nations in this area have used spyware to monitor journalists, opposition and dissidents.

1.3.1. Intrusions Against ICSs

This area has a long tradition of intrusions against ICSs and cyberphysical systems. These systems merge ICT and operational technology, OT, to monitor and control a production plant. Intrusions against an ICS can impact physical processes or activities.

The first intrusion is related to Stuxnet [52], which in 2010 targeted programmable logic controllers, PLCs. It is believed to have substantially damaged the nuclear program of Iran.

Attacks against ICSs are typically designed to directly alter, damage, or disrupt an industrial plant. Yet the most significant of these attacks to date reveals more worrying ambitions because, instead of seeking immediate disruption, they try to undermine a fundamental aspect of the integrity of the overall process to achieve impacts far greater than simply shutting down a plant or stopping the flow of electricity.

Attacks against oil and gas companies in the Gulf have mainly used wipers [18, 23, 36, 42]. Fig. 3 lists the wipers that have been used. Wipers are also among the most popular Russian cyber weapons in the invasion of Ukraine where several distinct wipers have been used to target critical and ICT infrastructures in coordination with physical attacks [35, 36, 42, 46].

Sabotage is the most obvious reason to deploy a wiper. Just as the Stuxnet [52] malware destroyed centrifuges in the Iranian enrichment plant of Natanz to slow the development of nuclear weapons, wiper malware could destroy data, sabotage development, cause financial loss or cause chaos. The Shamoon malware, used in 2012 to attack Saudi Aramco and other oil companies, destroyed 30,000 workstations at Saudi Aramco. This malware has been attributed to Iran.

A wiper can also be used to destroy evidence of intrusion or sabotage. After achieving their goals, such as espionage, the attackers simply deploy a wiper instead of meticulously erasing their tracks and all evidence. This not only erases the evidence, but the resulting destruction forces the defenders to focus on the recovery of data and operations and not on investigating the intrusion.

Name of the Wiper	Year	Target
Shamoon	2012	Saudi Aramco and Qatar's RasGas
Shamoon2	2016	Saud Arabian organizations
Stonedrill	2017	Saud Arabian organizations
Dustman	2019	Bapco, Bahrain's national oil company
ZeroCleare	2020	Energy companies in the Middle East

Fig.3. Some Wipers Used in the Gulf Region

When discussing wiper attacks against oil and gas ICS, it is worth recording that each ICS includes two subsystems separated by firewalls: the ICT subsystem and the OT one with SCADA/PLC, etc. The former is a standard ICT infrastructure with internet connections. It interfaces the devices in the OT subsystem against user applications, databases, etc. Wipers usually target the ICT system because the vulnerabilities of its standard components may be easily discovered. It is very difficult for a wiper to pass from the ICT system to the OT one. Currently, one of the few ransomware variants that target an OT subsystem is EKANS [17]. Several functional characteristics of EKANS are keyed to industrial environments but this variant has not yet been seen in the Gulf region.

[3] *A wiper malware damages an ICT/OT system by erasing or overwriting the information it stores.*

Despite incomplete information, another kind of attack against an ICS points out alternative solutions to force down a production plant. In mid-November 2017, Dragos discovered an ICS-tailored malware deployed against at least one victim in the Middle East [16]. The team identified this malware as TRISIS because it targets the Schneider Electric Triconex Safety Instrumented System (SIS), enabling the replacement of logic in final control elements. An SIS maintains safe conditions if other failures occur in critical production processes, and it provides life-saving stopping mechanisms. Compromising the security of an SIS does not necessarily compromise the safety of the system as long as its failure has no impact on the ICS. Hence, it is not currently known what exactly the safety implications of TRISIS would be. Logic changes on the final controller imply that safety may be at risk as set points could be changed. An SIS should be properly protected because even if an attack on it does not physically impact any element of the production plan, it can have multiple implications. The most likely scenarios are to create operational uncertainty and trip safety 'fail-safes' to halt operations. Manipulating the conditions to enter safety-preserving states during normal operations can force SIS-managed equipment to enter 'fail-safe' modes. This will likely stop the overall plant.

To cover other intrusions against ICSs, we list some intrusions against Iran that have been attributed to Israel and that may be seen as descendants of Stuxnet, as they target the Iranian uranium enrichment plant. Again, these cyberattacks against ICSs result in physical destruction [9]. On 01 July 2020, a cyberattack caused a fire and explosion at a new centrifuge production facility in Natanz. According to Israel, this was in response to a cyberattack by Iran that was intended to poison Israel's water supply by raising the chlorine levels. The damage could not be repaired, and on 08 September 2020, Iran announced that it would build a new, larger facility deep in the mountains near its Natanz nuclear site. On 27 June 2022, the Predatory Sparrow group carried out cyberattacks against three Iranian steel companies where they stole sensitive data. In the attack against the Khouzestan Steel Company, the group caused a fire by accessing the SCADA system that controlled the furnaces of the plant.

Israel is not the only target of Iran, which has a long tradition of cyber intrusions against the US as confirmed by the recent attribution by several US agencies to Iran of operations against the campaigns of both U.S. presidential candidates and targeting the American public with influence operations aimed at fanning political discord.[4] According to [2], Iranian threat actors began to develop tools and conduct campaigns in 2007, and their intrusions targeted more than a dozen U.S. companies and the U.S. Departments of Treasury and State.[5] The private sector victims of these actors are primarily targeted defence contractors. The US government has attributed some of these intrusions to actors working with companies affiliated with the Iranian Government Islamic Revolutionary Guard, IRGC. Microsoft lists more than ten groups that in Microsoft terminology share the name of "sandstorm". Other terminologies refer to the groups as "kittens". Due to obfuscation techniques, and government control over the Iranian media and internet, there is no insight into which group is Ministry of Intelligence vs IRGC. There is a consensus that each of these groups is rather small.

1.3.2 Ransomware Intrusions

According to recent data, even ransomware is a growing threat in the Gulf Cooperation Council (GCC). In 2023 more than 150 companies were targeted in the Middle East and 42 in GCC where Saudi Arabia and UAE were most impacted. Delving into the realm of ransomware in the GCC exposes an environment full of dangers for companies in the region, specifically Saudi Arabia and the UAE. Other recent ransomware reports state that 21% of Kuwaiti and 10% of Qatari companies were victims of these attacks, highlighting the vulnerability of regional organizations to these intrusions [1].

In 2023, data belonging to 53 companies based in the countries in GCC were published on ransomware-dedicated leak sites on the dark web. This is the number of attacked companies that did not pay the ransom. Therefore, it is also a lower bound on the number of companies that have been attacked. This approximation is not accurate, as it may miss several victims. As several experts

[4] *https://www.reuters.com/technology/cybersecurity/us-says-iran-cyber-operations-targeted-trump-harris-campaigns-2024-08-19/*
[5] *https://www.justice.gov/opa/pr/iranian-national-charged-multi-year-hacking-campaign-targeting-us-defense-contractors-and*

point out, the cultures of some nations in the GCC are sensitive to public shaming by ransomware gangs and there is a big loss of reputation for a Middle East company that is listed on a dedicated leak site. Therefore, some victims pay the ransom to avoid being publicly shamed by gangs.

Ransomware has emerged in the GCC due to the fast digitization of the region and the ever-changing cybersecurity landscape, which forms the basis for other reasons to emerge:

• Profitable Target,

•Rising Technology Dependence and Digitization,

• Rising Intricacy of Ransomware Methods: Ransomware operators continuously update their techniques to make them more effective.

An analysis of information related to financial entities on the dark web shows that 22% of all advertisements offer access to the infrastructure of organizations in different sectors. Access and data are highly related because attackers acquire access to the infrastructure of a company and use it to infiltrate the infrastructure to perform further attacks. As a result, attackers may gain data that is later sold on forums or distributed for free.

PART II

1. Regulatory/legal frameworks of the Cyber domain.

After discussing the ability to build cyber intrusions into adversary infrastructures, we consider increasing robustness and resilience. One of the tools for a state to improve robustness and resilience is the legislation concerning cybercrime and the protection of personal data. With a few exceptions such as Syria, Libya, and the state of Palestine, all the states in MENA have these legislations [49].

Thirteen Arab countries in MENA have passed specific legislation to combat cybercrime, while the rest have applied existing rules to these new crimes. Several experts believe that there are provisions in several laws that are incompatible with international treaties and conventions, resulting in a conflict in practical applications. The same experts believe that cybercrime and media legislation in Arab countries impede dialogue and curb freedom of expression. As an example, in Egypt, every personal website, blog, or social media account with more than 5,000 followers must be officially licenced following the law regulating the press and media. The 2012, UAE cybercrime law criminalized anyone who publishes information, news, statements or rumours on a website, computer network or information technology outlet to make sarcastic remarks towards or damage the reputation, prestige or stature of the State or any of its institutions. Further examples can be found in the laws of Jordan and Saudi Arabia. To apply these laws, states use state-of-the-art web scraper tools[6] that automatically analyse websites to discover and extract sentences with words/ sentences in a predefined list.

Data protection laws in Algeria, Egypt, Mauritania, Morocco and Tunisia are similar and have adopted the basic standards and data protection values as the European General Data Protection Regulation, GDPR. However, there are divergences, such as the mandatory registration of data, the omission of the 'transparency principles', or the power of a judge to give consent on behalf of a minor in Tunisia and Algeria. In addition, and especially, a transfer of data subject rights to heirs is an aspect that is not explicitly present in the EU data protection. In Algeria, Mauritania, and Tunisia, family members of a deceased person can 'inherit' and enforce the data protection rights of the deceased.

Within the last few years, Middle Eastern privacy legislation has drastically expanded in scope and power, owing a significant amount of influence to the GDPR, as evidenced by the provisions that closely reflect those in the GDPR. However, the new Middle Eastern privacy laws remain extremely protective of local data, possibly due to the still-expanding nature of Gulf economies and their dependence on a narrow range of economic sectors, most notably petroleum.

In the Middle East, recently Saudi Arabia, the United Arab Emirates and Bahrain passed data privacy and protection legislation, which

[6]Web scraping or web data extraction extracts data from websites. Web scraping software may access the World Wide Web using HTTP or a web browser. Web scraping can be implemented manually, or the process can be easily automated using a web crawler.

has demonstrated an increased commitment to consumer rights, business interests and the protection of personal information of the respective citizens of these nations.

Several free-trade zones in the GCC such as the Dubai International Financial Centre, the Abu Dhabi Global Market, and the Qatar Financial Centre have different cybersecurity regulations, mainly focused on data protection. They aim to ensure that businesses in these zones can work internationally, and they explicitly claim to follow international regulations, especially those of the European Union.

In Israel, businesses operating in areas of infrastructure that the state defines as "vital", which include telecommunications, water, electricity and transportation, are subject to binding state intervention. The directives themselves are then applied and enforced by the relevant ministry or authority. Private companies that operate in areas not classified as 'vital' but that the state considers strategically important are subject to sector-specific supervision managed by the appropriate ministries or by a private company subcontracted for this task. Cybersecurity in the rest of the private sector, however, is not regulated by the state but by the Privacy Protection Law, which requires organizations that own, manage, or store databases of personal information with more than 10,000 records to implement cybersecurity measures, which vary by the size of the database.

In the Gaza Strip, internet governance shadows the one in place in the West Bank: relying on Israeli infrastructures, Palestinian ISPs (Internet Service Providers) deliver the service across the Hamas-controlled region. In the absence of regionally controlled infrastructure networks and with extensive obstacles to regulating service delivery, the Hamas-led government retains marginal powers over its national cyber security.

A preliminary conclusion of data privacy protection and regulation is that the European approach to may not become a general standard in the MENA, where each nation will create a hybrid system according to distinct cultures and social ecosystems. Most countries prefer a more authoritarian approach to regulations, laws, and participation in international institutions, placing them in a category similar to those of proponents of cyber sovereignty. This reflects the tensions in the relationships of these states with Western democracies and suggests that a binary understanding of global cyber norms is incomplete.

2. National Capabilities and Mechanisms to Counter Cyber Threats[7]

This section describes in some detail how to evaluate the various abilities of a state related to cyber. In particular, we refer to the National Cyber Power Index, NCPI [50]. The Belfer Center for Science and International Affairs of Harvard Kennedy School has defined this index to rank the cyber power of nations. NCPI conceptualizes cyber power as composed of some objectives that states will attempt to achieve in and through cyberspace. In addition to the traditional perception of cyber power that only considers the ability to destroy and disable an adversary's infrastructure, states also seek to strengthen national cyber defences, gather intelligence, improve cyber and commercial technology know-how, control and manipulate the information environment, and influence international standards and norms. This results in the definition of eight objectives:

• Strengthening and Enhancing National Cyber Defence,

• Destroying or Disabling an Adversary's Infrastructure and Capabilities,

• Controlling and Manipulating the Information Environment,

• Foreign Intelligence Collection for National Security,

•Amassing Wealth and/or Extracting Cryptocurrency,

[7] *For evaluating the national capabilities and attitudes to counter cyber threats, we use an index defined by some researchers at Harvard University. The index considers eight objectives a state may aim to achieve. Then, it uses 29 indicators that evaluate the intent, i.e. willingness, and the capability of a state to reach these objectives. An index is used which we believe can forecast the robustness and resilience of the ICT/OT infrastructures of the various states. A detailed evaluation of these indicators points out important differences between states in MENA.*

•Growing National Cyber and Commercial Technology Competence,

• Surveillance and Monitoring of Domestic Groups,

• Defining International Cyber Norms and Technical Standards.

At least the first four objectives are related to cybersecurity and resilience. They are also related to our fil rouge because they consider the ability of a state to defend its own ICT/OT infrastructures while penetrating those of the competitors. The second objective concerns not only the infrastructures of another state but also the dismantling of botnets that host the attack infrastructure of threat agents that another state sponsors. These four objectives are fundamental to evaluating the cybersecurity and resilience of a state. Even the surveillance and monitoring of domestic groups is related to cybersecurity but from the perspective of spyware deployment rather than from that of infrastructure protection [14, 47]. The eight objectives are evaluated through 29 indicators such as population on the internet, data protection, and cyberattacks attributed to the nation. Some of the indicators evaluate the capability of a state to reach certain objectives, others indicate the intent of the state to reach the objectives. The index is the average value of the product of intent and capability for each of the objectives.

The indicators have been collected or estimated for 30 nations both in 2020 and 2022. According to the 2022 results, the US is in the first position with a final score close to 42. The following ranking defines the relative cyber power of some nations in MENA:

•Iran is in 10th place with a score close to 15

•Israel is 19th with a score close to 12

•Saudi Arabia is 21st with a score close to 11

•Egypt is 23rd with score close to 9

At first sight the scores are very similar, but a more detailed analysis of the eight objectives the evaluation considers shows some differences. In fact, some nations are much more focused on monitoring internal groups than on infrastructure defence. This implies we cannot expect large resilience of their ICT infrastructures. Israel is among the top nations in the intent to collect intelligence, but Israel has a much better collection capability. Iran is one of the top five nations when considering the capability of destroying the attack infrastructures of other nations. Only Israel, Egypt and Saudi Arabia have a reasonable capability of defending their infrastructures, even if some intrusions in their infrastructures have been undetected for a long time.[8]

[8] *https://www.darkreading.com/cyberattacks-data-breaches/undetected-attacks-against-middle-east-conducted*

Compared to other indexes, we believe the NCPI offers a more realistic evaluation of the general attitude of a nation regarding ICT technology [27].

Of particular note is that, even after the establishment of the NCPI, Jordan has released a National Cybersecurity Framework that endorses Cyber Risk Quantification and Management and a risk-based outlook on cybersecurity for public consultation. A draft of the framework document by the National Cybersecurity Center of Jordan states a goal to "promote the concept of Cybersecurity Economics to help every organization develop a sophisticated, economically driven" cyber risk management program. The framework encourages Jordanian organizations to graduate from qualitative risk assessments that "do not rely on precise and consistent definitions of risk, instead measuring it in terms of high-medium-low, red-yellow-green, or ordinal scales. Risk management and decision making based on qualitative risk assessments are fundamentally incorrect and erroneous because they are vulnerable to subjectivity." This perspective is rarely employed in other parts of the world.[9]

3. Cyber Capability: Gaps to Maintaining Resilience and Fighting Cyber Threats

We discuss possible actions to cover the gaps and improve resilience and fight cyber threats. Without a doubt, until now all efforts by individuals, nations, international organizations and private companies to improve the cybersecurity status have had little effect. Legislation on cyber security, thousands of penetration tests, user awareness training, and the adoption of many security tools have a minimal impact on cybersecurity.

This section describes some strategies to improve overall cyber security and resilience. Each of these strategies is related to one of the two abilities to increase robustness at home and build successful intrusions against adversaries.

[9] *https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/national_cyber_security_strategy_2018_2023.pdf*

3.1. Industry partners in MENA

Public/private cooperation with technology and insurance companies may be important to increase robustness and resilience as well as to build intrusions.

3.1.1. Technology Companies

The public/private partnership has produced important successes in the recent Ukrainian war, where major technology companies have become significant players in the conflict under the pressure of the Russian invasion. The cyber and information aspects of the current conflict are heavily dependent on private commercial organizations rather than on national resources. Providers of cybersecurity services, network components, software, cloud services and much more are all directly involved. Public and private partnerships, mostly those that cover cybersecurity and related sectors, can also improve intelligence to build future intrusions due to the huge amount of data and signals that some companies can access and analyse to discover anomalies.

Concerning public-private cooperation, it should be noted that the most noticeable example of successful cooperation is the state of Israel, which has the most start-ups per capita of any country, and that earned it the title 'start-up nation'. A large percentage of Israeli start-ups are focused on cybersecurity. The Israeli government has been continuously looking for ways to stimulate the growth of the tech ecosystem, and the programs it built to accomplish it turned out a great success [43].

The Israeli start-ups offer tools and solutions to increase robustness and resilience as well as to attack other infrastructures. Long before the recent rapprochement, Israel has successfully offered its cyber security tools to the Gulf monarchies [28]. In 2007, the UAE recruited the Israeli-owned US-based firm 4D Security Solutions to help increase the defence capacity of sensitive energy facilities and to establish a 'smart' surveillance system throughout Abu Dhabi. Following the Abraham Accords in 2020, UAE-Israeli cyber cooperation has witnessed major advancements.

3.1.2 Insurance Companies

Companies in MENA are well aware of the importance of cyber insurance. According to a 2022 survey by Marsh and Microsoft, 50% of surveyed organizations stated that "it is a best practice/ standard in our industry to have cyber insurance" while 54% claimed "we cannot cover all of the potential costs of a cyber incident without insurance." This is a strong indicator of the interest of organizations to adopt cyber insurance. It is expected that the cyber security market in the Middle East will increase at the compound annual growth rate of 10.38% till 2028. Insurance companies are further private organizations that may play an important role in private/ public cooperations. One main issue that has reduced the market for cybersecurity insurance is the complexity of predicting the probability of a successful intrusion against the system to be insured. Furthermore, several analysts believe that cyber risk is so widespread, unpredictable, expensive and unavoidable that private sector insurers cannot manage and pay for it alone but instead need assistance from the government. This kind of assistance has recently been refused by the UK government.[10] The insurance market could favour the spreading of good practices and solutions to increase both ICT robustness and resilience. Several companies offer tools that allow their customers to benchmark themselves against best practice standards and provide each user with a report including explanations and tips on how to improve their cyber risk posture. Furthermore, insurance companies can work with third-party data providers, service providers and model vendors to improve data quality and quantity, better understand risks, develop risk quantification and further advance modelling. The national cybersecurity framework by Jordan is an important step in the direction of decisions based upon risk quantification.

3.2. Working on the ICT/OT Ecosystem to Defend ICS

When moving from the actors to improve the robustness and resilience of infrastructures to the strategies to achieve these improvements, the two main issues are the ecosystem nature of the ICT/

[10] *https://bindinghook.com/articles-hooked-on-trends/insurers-will-help-define-the-threshold-for-cyberwar/*

OT environment and the still ambiguous nature of ransomware intrusions.

Defeating intrusions against ICS systems is one of the main goals of some nations in MENA. This is the same goal as that of some European directives. Understanding the evolution of the EU directive on critical infrastructure is important to avoid repeating those errors that have slowed down the increase of robustness and resilience of European critical infrastructure. An important notion when increasing the robustness of a critical infrastructure is the one of the ICT/OT ecosystem. The ecosystem nature of the ICT/OT environment implies that even attacks on some minor entity may impact the overall robustness and resilience. The importance of considering an ecosystem rather than a single infrastructure or a single company has been stressed by the increasing number of supply chain attacks. In these attacks, a threat actor targets a supplier of the real, or final, target to hide some malware in the products that the supplier will deliver to the real target that will install/connect it to its ICT/OT infrastructure. After this, the threat actor can exploit the malware to access and manipulate the infrastructure of the final target. Similar attacks can be implemented against open-source software [31, 45] because many of the package repositories for open-source languages are community-maintained, meaning the reporting and removal of malicious packages happen voluntarily rather than as the result of automated detection.

An effective defence against supply chain attacks requires that severe security requirements on organizations managing critical ICT infrastructures about the handling of these infrastructures, their monitoring, and the discovery and report of intrusions should be paired with equivalent requirements on their suppliers. This is one of the reasons the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, known as NIS 2, has replaced Directive (EU) 2016/1148 known as NIS. Both NIS and NIS 2 aim to improve the security of critical ICT infrastructures with the exclusion of those of financial organizations that are covered by the Digital Operational Act, DORA. NIS 2 expands its EU-wide security requirements and scope of covered organizations and sectors to improve the security of supply chains, simplify reporting obligations, and enforce more stringent measures and sanctions throughout Europe.

In the US, the Cybersecurity and Infrastructure Security Agency, CISA, is advancing the Software Bill of Materials, SBOM, as a key building block in software security and software supply chain risk management. An SBOM is a nested inventory, a list of ingredients that make up software components.[11]

3.3. Defeating Ransomware Gangs

Our discussion of how to face ransomware intrusions mostly uses information about Russian gangs. The first reason is that some intrusions against the ICS system in the MENA region have been attributed to these gangs. Furthermore, the evolution of the Russian ransomware gangs results in the worst case to be considered to defeat these gangs and, last but not least, a good amount of information on these gangs and their relation is available. When analysing ransomware gangs and their intrusions, we consider the gang ecosystem that is populated by at least four kinds of gangs:

1. Developers: they develop the malware to deploy to crypt the information in an infrastructure and receive the ransom;

2. Initial access broker: they sell information to penetrate an infrastructure;

3. Affiliates: they acquire the malware from a developer and access to the infrastructure from a broker to deploy the malware in the infrastructure and cash a percentage of the ransom that is paid to the developers;

4. Negotiators: they negotiate the ransom with the victims and manage the shame site, i.e. the dark web site to publish stolen information if the ransom is not paid.

The existence of an ecosystem with distinct species implies a high specialization of the

[11] *https://www.cisa.gov/sbom*

various gangs, which results in a stream of more effective and sophisticated malware. Defeating ransomware intrusions poses some interesting issues because, for one thing, the technical countermeasures to adopt are well known. Any report on a new gang or a new ransomware variant lists the same countermeasures that the victim should have applied before the intrusion to defeat the gang. The two countermeasures that are always present are network segmentation, i.e. splitting a network into subnets separated by firewalls, and multi-factor authentication. Zero-trust is another countermeasure with increasing popularity. Until now, very few public and private organizations have restructured their ICT/OT infrastructures according to these principles. Hence, an alternative solution is to defeat the criminal gangs that implement these intrusions.

To defeat the gangs, we first need to understand the members of the various gangs and their final goals. Several analyses have shown that there are no rigid boundaries among gangs because people migrate from one gang to another. Evidence of this migration is given by the code modules in the ransomware variant a gang uses that later appear in the variant of another gang. Significant law enforcement actions have recently destroyed major ransomware gangs like LockBit, and larger gangs have decreased their attack frequency to avoid detection. However, this has shifted the spotlight to smaller groups, which are now stepping up their activities. This makes smaller groups more active and prolific.

Another interesting point is that recent news confirms that some gang members work for Russian intelligence during work hours and for criminal gangs in their free time.[12] Furthermore, some researchers have confirmed that Russia-based ransomware groups increased their intrusions before elections in several major democracies, and companies that curtailed operations in Russia after the invasion of Ukraine were more likely to be targeted by these groups [34, 38, 39].

All the previous considerations suggest potential political motivations behind ransomware

[12] *https://analyst1.com/absolute-ransom-nation-state-ransomware/*

intrusions[13] or that Russian ransomware gangs are "tools of the state".[14] Therefore, ransomware may be considered a tool of hybrid war rather than a criminal phenomenon. Hence, the war against gangs should adopt another perspective [7] because the use of ransomware as part of cyber espionage activities may result in its misattribution as financially motivated operations. To further misguide attribution, APT (Advanced Persistent Threat) groups may purchase ransomware from cybercriminal actors. Ransomware also provides cover for the true motive behind cyber espionage operations and data exfiltration. Cyberespionage disguised as ransomware also offers an opportunity for adversarial countries to claim plausible deniability by attributing the actions to criminal gangs.

3.4. Spyware

The indicators to compute the National Cyber Power Index in Part II, Sect. 2.2 show that some states in MENA have a strong interest in spyware to monitor groups of opposition. This is confirmed by the long tradition of spyware in the region that is used to support government or approved public figures, to counter anti-government views, or to distract attention from certain themes. A survey has revealed that at least 23 companies provide surveillance technologies to governments in the MENA region, particularly European, North American, Chinese and Israeli firms.[15] According to some sources more than half of the intrusions against individuals in the Middle East involved spyware.[16] As an example, in July 2024 more than 450 military personnel from Middle East countries have been the target of an ongoing surveillance ware operation that delivers GuardZoo, an Android data-gathering tool. The campaign, believed to have commenced as early as October 2019, has been attributed to a Houthi-aligned threat actor. The targets of the malicious activity were located in Egypt, Oman, Qatar, Saudi Arabia, the UAE, and Yemen. According to telemetry data, most infections have been recorded in Yemen.[17] Despite rising integration, the Houthi-Iran relationship is not a classic patron-client because the Houthis often behave like a proxy but with their agenda, and notable agency. The New York Times reported in 2022 that the NSO Group charged customers $500,000 just to install the Pegasus spyware and $650,000 to get into 10 devices. The report also said that infiltrating 10 Android devices would cost an agency $650,000 and the same cost would apply to 10 iPhone gadgets.[18]

There is a strong connection between spyware and robustness because, from a technical point of view, the deployment of spyware on a device requires and exploits vulnerabilities in the target device. In most cases, some of these vulnerabilities are zero days, i.e. they are not public. A state that is strongly interested in spyware or botnets cannot reveal the existence of some vulnerabilities or remediate the ones it exploits in its surveillance. This leaves some weak points in the overall ICT/OT ecosystem that can be exploited not only for surveillance but also to build intrusions. As an example, Hacking Team was a very active company in the spyware field in the Middle East and they relied on a number of zero-day vulnerabilities. When Hacking Team was hacked, its library of zero days was disclosed and subsequently used by threat actors around the world in their intrusions.

3.5. Being Proactive from the Outset

Proactivity is an important attitude to increase the resilience of any ICT/OT infrastructure. Experience has shown that improving an ICT/OT infrastructure only after it has been attacked is dangerous for overall security and also much more expensive because, as the GDPR points out, the cheapest security is security by design. Security by design means that possible intrusions should be anticipated by analysing the intrusions a threat agent can implement against a system before building the system. Even standard and well-known countermeasures, such as network segmentation,[19] defence in depth, and multifactor authentication can largely improve the resilience of a system with a minimal cost, provided they are

[13] *https://theweek.com/politics/russia-waging-hybrid-war-against-west*
[14] *https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf*
[15] *https://www.business-humanrights.org/en/from-us/briefings/mena-surveillance-2024/*
[16] *https://www.ptsecurity.com/ww-en/about/news/pt-most-attacks-on-individuals-in-the-middle-east-involve-spyware/*
[17] *https://thehackernews.com/2024/07/guardzoo-malware-targets-over-450.html*
[18] *https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html*
[19] *https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-193a*

adopted in the design step rather than as an overall expensive restructuring of an infrastructure.

Another example of weak design is related to the proliferation of security tools in both ICT and ICT/OT infrastructures. The paradox here is that there are some attack techniques, such as "living off the land",[20] where attackers acquire control of these tools and then use the large set of access rights these tools are granted against the system the tools should protect. Recently, attackers have used end-point protection tools that can kill dangerous applications or malware to kill other defence tools and destroy backups.

Besides a weak and cheap design, another source of security problems is the forecast of future intrusions using historical data, i.e. data on those that occurred in the past. This neglects that cyber risk scenarios are highly dynamic, as confirmed by the rapid evolution of tactics, techniques, and procedures of attackers and by the quick development of new variants of malware. The resulting drift of historical data on intrusion is a source of risk that is too often neglected and results in a false sense of security because it assumes that attackers will behave as in previous intrusions. Discovering how new attack techniques and new ransomware variants can affect an infrastructure before an intrusion occurs is the current main challenge for defenders [3,4,5,32].

[20]When adopting "living off the land" techniques, attackers use tools already installed on a system rather than deploying their own tools. This minimizes the probability the defenders can detect the intrusion.

CONCLUSIONS AND RECOMMENDATIONS TO NATO

Cybersecurity is a highly dynamic and technology-driven phenomenon. Hence, most of the recommendations proposed in the following are valid worldwide rather than in MENA alone. We believe this cannot be considered as a detracting factor for the recommendations contained herein, due to the spreading of the underlying technologies and the simultaneous rapid spreading of intrusion and attack techniques.
Our five recommendations have a strong technological background. They aim to exploit the supranational nature of NATO to sustain the adoption of proper technical solutions to improve robustness and resilience of ICT/OT infrastructures in the region.

1. Support vulnerability disclosure and management

a) Improve the robustness of ICT/OT infrastructures

As long as a large number of vulnerabilities are not public, the overall robustness and resilience of ICT/OT infrastructures are at risk because even a few vulnerabilities can enable intrusions with huge impacts mainly when the target is an ICS.[21] The resulting fragility of infrastructures is the most dangerous side effect of building an arsenal of zero-day vulnerabilities because they may be used against those who built the arsenal as it happened in the past. This is strongly related to spyware diffusion that strongly exploits zero day.

[21] The idea that users are safer when bugs are kept secret is called "security through obscurity".

b) Do not leak weapons to adversaries

Any intrusions that exploit a zero-day vulnerability deliver a weapon to adversaries because in cybersecurity, most victims know, or can learn, how to reuse the weapons that have been used against them. In MENA, Iran is the best example of this ability as well as of learning from the attacks that have targeted this state. The acquired capabilities can be uses not only in MENA but also against other nations. Hence, building an arsenal of zero-day privileges the ability to implement intrusions that penetrate ICT/OT infrastructures and spread spyware at the expense of robustness. A better balance may be the public disclosure and remedying of vulnerabilities in a transparent way.

c) Develop and validate tools to manage vulnerabilities

NATO could adopt and favour the adoption of methodologies and tools to manage information about vulnerabilities and their public disclosure to improve robustness and resilience in the life of a system from design to dismission. The expertise of NATO and its various centres could be fundamental to ensuring the quality of tools to discover, rank and remove vulnerabilities. This is a field where cooperation with private companies and insurance may act as a strength multiplier for NATO efforts.

2. Cooperate to dismantle attack infrastructures

NATO should play a fundamental role in supporting states to reach a good compromise between increasing robustness and building successful intrusions to dismantle the attack infrastructure of gangs and enemies.

a) Contrast hybrid threats

The destruction of attack infrastructures may enable NATO to win one of its most pressing challenges – that of hybrid cyber threats. The Alliance faces a barrage of malicious cyber activities from all over the globe, due to state-sponsored actors, hacktivists and criminals. These attackers are willing to cross lines and execute intrusions that were previously considered unlikely or inconceivable. In addition to military targets, NATO must consider the risks that malicious activities of hybrid threats pose to hospitals, civil society, and other targets, which could impact resilience in most countries.

b) Defeat ransomware gangs

Among hybrid threats, a particular role is played by ransomware gangs that should be dismantled if it can be proved that ransomware is an act of hybrid warfare rather than a simple criminal activity. Dismantling the gangs implies the coordinated destruction not only of attack infrastructures but also of internet domains and botnets, a problem that also arises when fighting the spreading of fake news. These operations require international cooperation. In turn, this results in several requirements and constraints of law enforcement operations. The role and strength of NATO can be fundamental in these operations as well as in supporting smaller and less powerful nations, such as several of the Mediterranean region. This can also be critical to strengthening political dialogue and practical, more fruitful cooperation with nations in the Gulf area where public and private institutions are interesting and fruitful targets for ransomware intrusions.

3. Define standards and best practices for equipment acquisition, management and dismissal

Besides supporting the security by design approach guideline, NATO should adopt clear general rules for acquisitions where a fixed percentage of development costs of the supply or service should be allocated for cybersecurity and resilience testing and evaluation. Furthermore, to achieve a secure supply chain a system bill of materials should be produced for each of the various modules. The stress tests to evaluate robustness and resilience should be clearly defined in the call for tender and applied to the final supply or service. This will result in best practices for acquisition that could be spread to nations and private organizations. The overall goal is to shift the liabilities of security problems from the final users to the producers.

4. Favor robustness with respect to resilience

Currently, there is a large attention on increasing resilience as the most cost-effective approach against cyber intrusions. Anyway, no one should forget that in several cases robustness is the most important property because, as attacks against ICS/OT infrastructures teach, there is no way of recovering the physical impacts of some intrusions. Defining methodologies to build robust systems from modules with some vulnerabilities is an important step to minimize the cost arising when replacing robustness with resilience.

5. Increase cooperation with the private sector

NATO should use the know-how and the abilities of the private sector in the same way as it uses those of its constituent members. The war in Ukraine is the first important example that has confirmed that the difference between worldwide organizations and states may be minimal. Outside a war scenario, cooperation requires proper legal frameworks and international treaties due to the international nature of criminal gangs. Supranational organizations play an important role in creating and improving these frameworks that always require a sound technological basis [13, 31, 35, 36, 41]. Furthermore, the power of private partners offers NATO the opportunity to be proactive in cyberspace.

REFERENCES

1. Al-Mulhim, R. A., Lama A. A., Fay M. A. Cyber-attacks on Saudi Arabia environment, International Journal
of Computer Networks and Communications Security 8.3 26-31, 2020.

2. Anderson C., Sadjadpour K., Iran's Cyber Threat: Espionage, Sabotage, Revenge. Carnegie Endowment for International Peace,
https://carnegie-production-assets.s3.amazonaws.com/static/files/Iran_Cyber_Final_Full_v2.pdf.

3. Baiardi, F., Tonelli, F. Twin-based continuous patching to minimize cyber risk. European Journal for Security Research, 6(2), 211-227, 2021.

4. Baiardi, F. A Framework for ICT Resilience. In Resilience and Hybrid Threats 27-42, NATO Science for Peace and Security Series - D: Information and Communication Security, ios press, 2019.

5. Baiardi F. et al. Anticipating Disasters through a Security Twin International Workshop on Dynamics of Disasters: Hybrid Threats (Vienna, Austria), Aug. 2024.

6. Beek K., Africa Ranks Low on Phishing Cyber Resilience, https://www.darkreading.com/vulnerabilities-threats/africa-ranks-low-on-phishing-cyber-resilience, June 2024.

7. Bátrla, M., & Harašta, J. 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In 2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon) (Vol. 700, pp. 93-115). IEEE, 2022.

8. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., Varese, F. Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one, 19(4), e0297312. (2024).

9. Caruso, J. Inside Cyber Warfare. Third edition, O'Reilly, Oct. 2024.

10. Chainalysis, The 2023 Geography of Cryptocurrency Report 2023, https://www.chainalysis.com/wp-content/uploads/2024/06/the-2023-geography-of-cryptocurrency-report-release.pdf.

11. Cho, S. Enhancing Cyber Security of Industrial Control Systems, Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency, Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022.

12. ClearSky, Infrastructure and Samples of Hamas' Android Malware Targeting Israeli Soldiers. Cambridge: Clearsky Security Ltd., 2018.

13. Córdova, Kim, Schneier.B. The Hacking of Culture and the Creation of Socio-Technical Debt, e-flux Journal, June 13, 2024.

14. Council of Europe, Pegasus and similar spyware and secret state surveillance, https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68, 20 Sept. 2023.

15. CrowdStrike, Global Threat Report, 2024.

16. Dragos, TRISIS Malware- Analysis of Safety System Targeted Malware, https://www.dragos.com/resources/whitepaper/trisis-analyzing-safety-system-targeting-malware/ 2017.

17. Dragos, EKANS Ransomware and ICS Operations https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/, March 2020.

18.Dragos, OT Cybersecurity Year in Review 2023, 2024.

19. ENISA Threat Landscape for Ransomware Attacks, July 2022.

20. Finckenstein, V. Cybersecurity in the Middle East and North Africa, Konrad Adenauer Foundation Lebanon Office, July 2019.

21. Fuentes, M.R. Digital Souks: A Glimpse into the Middle Eastern and North African Underground, TrendLabsSM Research Paper, 2018.

22. Group-IB, High Tech Crime Trends Report, 2023-2024, 2024.

23. Greenberg A.. “The untold story of NotPetya, the most devastating cyberattack in history.” Wired, August 22 (2018).

24. IBM Security, Cost of a Data Breach 2023, https://www.ibm.com/downloads/cas/E3G5JMBP, 2024.

25. Interpol, African Cyberthreat Assessment Report 2024, Outlook by the African Cybercrime Operation Desk, March 2023.

26. Interpol, African Cyberthreat Assessment Report 2024, Outlook by the African Cybercrime Operation Desk - 3rd edition, April 2024.

27. United Nation’s International Telecommunication Union Pubblications, Global Cybersecurity Index 2020.

28. Jones, C., Guzansky, Y, Fraternal enemies: Israel and the Gulf monarchies. Oxford University Press, 2020.

29. Katz, Y., Bohbot, A. The weapon wizards: How Israel became a high-tech military superpower. St. Martin’s Press, 2017.

30. Kerttunen, M. The Absolute Ideal: Military Capabilities in World and Society, WP N.03, German Institute for International and Security Affairs, June 2023.

31. Ladisa, P., Plate, H., Martinez, M., & Barais, O. Sok: Taxonomy of attacks on open-source software supply chains. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1509-1526). IEEE, May 2023.

32. Linkov, Igor, Baiardi F. et al. Applying resilience to hybrid threats. IEEE Security & Privacy 17.5 (2019): 78-83.

33. Malik, N. Terror in the Dark. How Terrorists Use Encryption, the Darknet and Cryptocurrencies, The Henry Jackson Society, 2018.

34. Martin, J., Whelan, C. Ransomware through the lens of state crime: conceptualizing ransomware groups as cyber proxies, pirates, and privateers. State Crime J., 12, 4, 2023.

35. Microsoft, Defending Ukraine: Early Lessons from the Cyber War, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, June 2022.

36. Microsoft Threat Intelligence, A year of Russian hybrid warfare in Ukraine: What we have learned about nation state tactics so far and what may be on the horizon, , https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf, March 2023.

37. Microsoft Threat Analysis Center, Iran surges cyber-enabled influence operations in support of Hamas, , https://aka.ms/IranReport-Feb2024, Feb. 2024.

38. Nershi, K., and Grossman S., Assessing the political motivations behind ransomware attacks, Available at SSRN 4507111, 2023.

39. Performanta, Cyber Warfare: Expert Analysis on Nation State Attacks, https://www.performanta.com/ebook-cyber-warfare, 2024.

40. Positive Technology, Cybersecurity Threatscape of African Countries, 2022-2023, July 2023.

41. Ryan M., Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Springer, 2021.

42. Recorded Future, Overview of the 9 Distinct Wipers Used in the Ukrainian War, May 2022.

43. Senor, D., and Singer S., Start-up nation: The story of Israel's economic miracle. Random House Digital, Inc., 2011.

44. Sonatype, 9th annual report on State of the Software Supply Chain, 2023.

45. Threat Analysis Group, Mandiant, Google Trust and Safety, Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflicttransformed-the-cyber-threat-landscape/, Feb. 2023.

46. Threat Analysis Group, Buying Spying: How the commercial surveillance industry works and what can be done about it, https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/ Feb. 2024.

47. Threat Analysis Group, Mandiant, Google Trust and Safety, Tools of First Resort: Israel-Hams war in the Cyber https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/, Feb. 2024.

48. UN Trade and Development, Global Cyberlaw Tracker, https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

49. Voo, J, Irfan H. and Cassidy D. National Cyber Power Index 2022, Belfer Center for Science and International Affairs, Harvard Kennedy School, Sept. 2022.

50. World Economic Forum, Global Cybersecurity Outlook 2024, Insight Report, https://www.weforum.org/publications/global-cybersecurity-outlook-2024/, Jan. 2024.

51. Zetter, K.. Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Broadway Books, 2014.

Sources consulted but not referenced

1. Denning, D. Stuxnet: What Has Changed?. Future Internet, 4(3), 672-687; https://doi.org/10.3390/fi4030672, https://www.mdpi.com/1999-5903/4/3/672, 2012.

2. Shires J., Hakmeh J., Is the GCC Cyber Resilient? Briefing, International Security Programme, Chatman House, March 2020.

3. London School of Economy, Global Strategies. Hybrid Warfare in the Middle East, LSE !ideas], Feb. 2017.

4. The European Centre of Excellence for Countering Hybrid Threats, Trends in MENA: New dynamics of authority and power, Research Report 7, June 2021.

5. Brigadier General Y.S. The Human-Machine Team: How to Create Synergy Between Human and Artificial Intelligence That Will Revolutionize Our World, independently Published, 2021.

6. The European Centre of Excellence for Countering Hybrid Threats, Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence, Hybrid CoE Research Report 5, March 2022.

7. The European Centre of Excellence for Countering Hybrid Threats, The relevance of Clausewitzian theory in hybrid war: The Iranian-Saudi rivalry, Hybrid CoE Working Paper 15, March 2022.

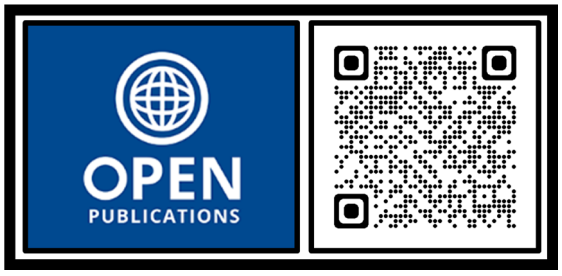
8. Loewenstein, A. The Palestine laboratory: How Israel exports the technology of occupation around the world. Verso Books, 2023.

9. World Economic Forum, The Global Risk Report 2024, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

10. Pelroth, N. This Is How They Tell Me the World Ends: The Cyberweapons Arms Race, Bloomsbury Publishing, 2021.

11. Campbell E., Sexton M, , Cyber War and Cyber Peace: Digital Conflict in the Middle East T - Middle East Institute Policy Series 2022 Bloomsbury Academic.

12. Byman D., McCaleb E. Understanding Hamas's and Hezbollah's Uses of Information Technology, Center for Strategic and International Studies Briefs, July 2023.



Cybersecurity in the Middle East and North Africa
www.openpublications.org