GCSP

GenevaPapers

Cybersecurity Challenges in the Middle East

22/17

Research Series

Dr Sameh Aboul-Enein

Cybersecurity Challenges in the Middle East

The Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation established in 1995, with 51 member states, for the primary purpose of promoting peace, security and international cooperation through executive education, applied policy research and dialogue. The GCSP trains government officials, diplomats, military officers, international civil servants and NGO and private sector staff in pertinent fields of international peace and security.

The Geneva Papers and l'Esprit de Genève

With its vocation for peace, Geneva is the city where international organisations, NGOs and the academic community, working together, have the possibility of creating the essential conditions for debate and concrete action. The Geneva Papers intend to serve the same goal by promoting a platform for constructive and substantive dialogue.

Geneva Papers Research Series

The Geneva Papers Research Series is a set of publications offered by the GCSP. It complements the Geneva Papers Conference Series that was launched in 2008, whose purpose is to reflect on the main issues and debates of an event organised by the GCSP.

The Geneva Papers Research Series seeks to analyse international security issues through an approach that combines policy analysis and academic rigour. It encourages reflection on new and traditional security issues that are relevant to GCSP training, such as the globalisation of security, new threats to international security, conflict trends and conflict management, transatlantic and European security, the role of international institutions in security governance and human security. The Research Series offers innovative analyses, case studies, policy prescriptions and critiques, to encourage global discussion.

Drafts are peer-reviewed by the GCSP Review Committee.

All Geneva Papers are available online at www.gcsp.ch/Knowledge/Publications

For further information, please contact: publications@gcsp.ch

ISBN: 978-2-88947-100-3

About the Author

Dr Sameh Aboul-Enein is an Expert Member of the United Nations Group of Governmental Experts (2014-2015) on Development in the Field of Information and Telecommunications in the Context of International Security.

For more information on the author, see
www.gcsp.ch/News-Knowledge/Experts/Fellows/Aboul-Enein-Amb.-Dr-Sameh-Aboul-Enein

The author would like to express his appreciation for the help of Research Assistant Nadine George Iskandar in the preparation of this paper.

The author has written this paper in his own academic and personal capacity.

Content

About the Author 6

Executive Summary 8

1. The new cyber era in the Middle East 9

1.1 The road towards digitisation and its dynamics 9

1.2 Constraints and limitations: domestic and foreign policy and regulation 9

2. Roadmap of challenges and obstacles 11

2.1 The economy 11

2.2 Education and the Internet gender gap 13

2.3 Cybercrime 16

2.4 Cyberterrorism, nuclear security and critical infrastructure 18

3. Middle East cybersecurity initiatives 23

3.1 Cyber surveillance of non-state actors 23

3.2 Cyber legislation 24

4. The way forward: a multilateral sustainable solution 27

4.1 Capacity-building 27

4.2 Diplomacy 28

4.3 Legislation 29

4.4 Establishment and implementation of norms 30

5. Conclusion 33

6. Recommendations 35

6.1 Promoting cybersecurity competence building at universities 35

6.2 Promoting competence building through professional training 35

6.3 Updating cybersecurity techniques and capabilities 37

6.4 Promoting a culture of cybersecurity 39

Endnotes 41

Geneva Papers – Research Series 48

Executive Summary

Countries in the Middle East are increasingly investing in information and communication technologies (ICTs). Social infrastructure, the financial sector, government services, schools, and hospitals in the region are now irreversibly dependent on interconnectivity and the Internet. At the same time, the role of ICTs has become an integral part of the future of domestic and international security architecture in the Middle East, emphasising the need for the development of effective cybersecurity at a regional level. The majority of global military powers have developed cyberwarfare capabilities and doctrines, and this will inevitably result in more states acquiring this capability in the near future. Non-state actors have also become highly proficient in exploiting cyber vulnerabilities.

This environment raises questions about the trends in cyberwarfare and offensive cyber tactics, the appropriateness of existing international humanitarian laws on the use of force in cyberspace, and the concomitant obligations of states and international institutions in managing all of this. This paper examines and addresses key challenges to cyber stability in the Middle East in the four areas of:

- economics;
- education and the Internet gender gap;
- cybercrime; and
- cyberterrorism and the threat to nuclear security.

It stresses the need for more cyber-related legislation, ICT education, and better defences against cyberterrorism and cybercrime. It argues for the promotion of a cybersecurity culture in the Middle East that focuses on individual, national and international security by including all essential stakeholders as the only way of effectively addressing the threat of cyberattacks in the region.

1. The new cyber era in the Middle East

1.1 The road towards digitisation and its dynamics

Governments, enterprises, and individuals in the Middle East are adopting connected digital technologies and applications on a massive scale in a process known as digitisation. The Middle East's digital markets are expanding at an overall compound annual growth rate of 12 per cent and could add as much as US$820 billion to gross domestic product and create 4.4 million new jobs by 2020.[1] Millions of home users joined cyberspace and social networking websites during the Arab Spring in 2011 and, according to statistics from the Internet World Stats database, in North Africa alone Egypt had 34.8 million Internet users, Morocco had 20.2 million, Algeria had 15 million, and Tunisia had 5.8 million in December 2016.[2] Social networks and web applications played a critical role in the 2011 uprising, profoundly affecting regional politics. These social media outlets offered an opportunity for people in the region to self-mobilise and create online communities, but they also increased the frequency and scope of cyberattacks, cybercrime, cyberterrorism, malware, digital espionage and violations of privacy. The worst outcome of this growth in Internet abuse would be that the "Internet breaks on our watch".[3] In this situation, the costs that would arise as a result of the activities of offenders and the simultaneous impact of greater government control of the Internet could increase to a point where people and organisations reduce their use of the Internet.[4]

1.2 Constraints and limitations: domestic and foreign policy and regulation

In response to the scenario described above, Middle East governments could begin to introduce constraints on cyberspace that further segment the Internet and might facilitate the abuse of essential human rights.[5] For example, individual freedoms and civil rights are under threat from increasing state cyber-tracking and monitoring capabilities, as well as the capacity to censor or shut down social networks and Internet connectivity. Equally, the growth in cyberattacks since 2011 has compromised state actors' power to protect systems, despite advances in cyber technology and software protection methods. Determined hackers can always find a way to target systems and remain one step ahead of the technologies designed to protect them, often with serious consequences for governments, corporations and individuals.

On the other hand, at the level of international relations, cyber technology is reshaping the way in which nations conduct their foreign policy and diplomacy. Innovations in ICTs are being used in diplomacy, while ICTs offer new opportunities for governments to interact with the public by utilising a network approach that embraces an increasingly multicentric, globally interdependent system.

2. Roadmap of challenges and obstacles

2.1 The economy

2.1.1 Banks and monetary institutions

According to a 2014 report, cybercrime is estimated to cost the global economy a reported US$400 billion annually.[6] At a conservative estimate, losses are at least US$375 billion, and in the view of some experts may be as high as US$575 billion.[7] El-Guindy estimates that the Middle East is a desirable target for many cybercriminals in terms of financial gain due to the poor awareness of many ICT users, the lack of technical ability and appropriate legislation, and the availability of cash.[8] Furthermore, cybercriminals target regions with poor or non-existent regulations to carry out their financial cyberattacks. Recent reports of attacks on banks in the region prove the devastating effects that cyberattacks can have on both the regional and global economy. In December 2012 and February 2013, respectively, RAK Bank in the United Arab Emirates (UAE) and BMI in Oman were targeted by an international gang of criminals. The gang was able to hack into the systems of card-processing firms and increase the available balance and withdrawal limits on pre-paid debit cards. They also coded fake cards and gave them to gang members around the world, who withdrew US$45 million from cash machines in 27 countries.[9]

Middle Eastern banks lag behind in their implementation of effective ICT data-security measures, and although financial institutions are working to improve policies and procedures to meet international standards, the implementation of these security measures is currently at a weak stage.[10]

Cybercriminals also target small entities in the region that deal with money due to gaps in these entities' security systems.[11] In addition, the growing use of mobile Internet in the Middle East and the increase of e-commerce sales are becoming major targets for cybercriminals.[12] Thus, it is important that citizens who might be affected by cybercrime understand the way in which private companies both store data and regulate data transfers.

2.1.2 The digital economy and world trade

As with local and regional trade, so with world trade. The modern world approaches international trade differently due to the rapid development of digital technology. As digital technologies become more affordable, the costs associated with transferring data have significantly decreased and profits have increased. Information and digital services can now be digitally transferred, while almost all business transactions rely on some form of digital management, for example, order-status tracking information, inventory records or employee data.[13] This data can be either transferred within a company or among companies, and at times a third-party data processor is used to make such transfers. Companies and individuals are developing faster ways to facilitate international digital transfers. Thus, a universal method of regulating the large number of cross-border data transfers is needed.

2.1.3 Data transfer regulation

There has been much debate over how to regulate international data transfers, and it brings with it many factors to consider such as those relating to storing, processing, and accessing large volumes of data from anywhere in the world.[14] It is just as important to securely transfer data as it is to store it. As data travels to its final destination it is critical that handlers ensure that personal data stays private during the entire transfer process. Any error by handlers can negatively impact the security of individual citizens.[15] In one case the national identification numbers, addresses, and telephone numbers of 50 million Turkish citizens were leaked.[16] This is not an isolated incident and there have been many more breaches of citizens' security, yet ordinary citizens remain unaware of how often their personal data is exposed, and it is this ignorance that keeps them from demanding greater privacy protection from their leaders. According to Sherif Hashem, vice president for cybersecurity at the National Telecom Regulatory Authority in Egypt, educating individuals is essential so that they know exactly what measures are being applied to protect their data, what type of data is being collected, and who has access to this data, even when it is the role of the regulator to make individuals feel secure in a way that is transparent.[17] Hashem stresses that the leaking of an individual's data not only puts the individual at risk, but also has economic and financial repercussions that could take months to deal with.[18] Possible measures to boost security include the use of encryption, secure channels and multifactor authentication to ensure that sensitive data is secure.

Another significant cost of cybercrime arises from its damage to company performance and national economies. According to Intel Security, cybercrime damages not only trade itself, but also innovation, competition and growth.[19] The majority of Middle East and North African countries rank high in international financial crimes statistics.[20] These statistics reveal that 26 per cent of businesses in the region report being the victims of economic crime, 30 per cent believe that cybercrime remains the second most reported economic crime affecting organisations, and 63 per cent indicate that opportunity is the main reason for criminals to commit economic cybercrime.[21]

Companies in the region are beginning to create solutions to block network breaches and cyberattacks, but cybercriminals are changing tactics to evade detection and continue to steal information. A study conducted by PricewaterhouseCoopers (PwC) in 2016 found that 21 per cent of respondents in the region did not know if they had been victims of cybercrime and over a quarter of those who admitted that they had suffered a cyberattack believed that there had been no financial loss as a result.[22]

These percentages are suspiciously low, given that 42 per cent of respondents in the region believe they have suffered high- or medium-level damage to their reputation as a result of cyberattacks, compared to 30 per cent globally.[23] Furthermore in PwC's 19th Annual CEO

2016 survey, 61 per cent of respondents admitted that they were concerned about cyber risk, yet only 39 per cent of Middle East boards in the survey asked for any information about their organisations' readiness to cope with a cyberattack and 12 per cent had not considered whether they needed to have such information.[24]

In addition, while the reported number of affected organisations in the Middle East is lower than the global average, the number in the region that were unaware that they were victims of cybercrime was 20 per cent, compared to the global average of 11 per cent.[25] This security concern is made more prominent by the fact that over 50 per cent of the organisations surveyed had not or did not know if they had conducted a fraud risk assessment during the previous two years.[26] When looking at the financial impact on the region, the losses are in the US$5 million-100 million dollar range and have gone up since the most recent PwC survey.[27] The increase in thefts of less than US$50,000 dollars indicates an increase in criminal organisations in the Middle East in 2014.[28] However, PwC considers that there was a worldwide decline in the misappropriation of assets, corruption, bribery, and procurement and account fraud, including in the Middle East, in 2016: and while cybercrime has increased globally and jumped by 32 per cent in 2016, up 8 per cent from 2014, the Middle East shows a decline in cybercrime of 7 per cent for the same period.[29]

The challenge for businesses, then, is to eliminate the opportunities for economic crime, which can be partly achieved by their remaining vigilant about new threats and finding new means of prevention, detection and response.[30] Businesses can prevent economic crime in general by ensuring that their organisations develop a culture based on shared values that are supported through an ethics and compliance programme focused on everyday decision-making.

2.2 Education and the Internet gender gap

2.2.1 Individual responsibility, awareness and Internet access

Cybersecurity is not just a national, but also a personal issue, and in order to improve national cybersecurity, the first step is to encourage individuals to take responsibility for their own online security. Individual citizens need to increase their cyber capabilities if they are to be active and engaged social agents. The Internet has engaged over three billion individuals in only a couple of decades; nonetheless, over half of the world's population remains unconnected. In the event that the rest of humanity is not given the chance to access the web, computerised and physical barriers both inside and between social orders will increase, locking many people into a permanent cycle of exclusion from an inexorably advancing world economy.[31]

These issues can be effectively addressed through the creation of training programmes for citizens of developing countries to help them overcome the digital divide and by adding

information security to the curriculum of all education systems at all levels in the region. To help deal with the problem of lack of access, governments should invest in and establish online access points that will allow the public to interact with the Internet.[32] Open Internet access ought to be made available in schools, libraries and other social administration venues to guarantee that people are not kept from the benefits of Internet access due to a lack of the necessary equipment.[33]

2.2.2 Gender frameworks, rehabilitation, training and knowledge sharing

A few awareness campaigns are currently in place in Oman, Saudi Arabia, Qatar and the UAE.[34] Education and awareness are integral to combating cyber threats, thus there is a need to improve capacity-building and the education of employees and citizens. One proposal has arisen through UN Women and its programmes for Syrian refugee women. Currently the organisation's aid efforts focus on the economic empowerment of Syrian refugee women in their communities, and while this is vital, educating these women in cyber technologies and the rapid developments in the field of cybersecurity is also important. These women have been at the forefront of the struggle to protect civilians, enhance livelihoods, address the needs of victims and survivors, and promote diplomatic activism.[35] However, the evolution of the Syrian conflict from an uprising to an armed conflict involving many national and international actors shifted attention from the causes of the conflict to its consequences, and this caused people to portray women as victims rather than active agents who, if given the opportunity and skills, can develop strong policies and strategies to, among other things, combat cybercrime in their region.

One reason that confirms the need to offer an ICT curriculum to refugee women and provide them with cyber capabilities is that the new ICTs have provided a platform for cultural norms and patriarchal modes of interaction, leading to the reproduction of gender violence.[36] A recent report released by the UN Broadband Commission states that 75 per cent of women online had been exposed to some form of cyber violence.[37] Online abuse of women includes hate speech, hacking, identity theft, and online stalking, and can also extend to human trafficking.[38] In fact, the demand for human trafficking overall allows traffickers to use the legal aspects of commercial sex on the Internet as a cover for their illegal activities. This violence is reminiscent of the abuse that Syrian refugee women faced and are currently enduring as they flee to refugee camps. The International Federation for Human Rights, in collaboration with the Arab Women Organisation, sent an international fact-finding mission to Syria to investigate violence committed against women during the ongoing conflict.[39] Of the 80 refugee women who were interviewed, all reported having witnessed or heard about cases of sexual violence and said that the fear of being assaulted motivated them to leave their country.[40] Women who were interviewed gave indirect accounts of assault cases during house searches, after being arrested at checkpoints and while they were in detention.[41] The risk of survivors of attacks being rejected by their communities imposes a culture of silence among

the majority of women, and it is precisely this silence that makes possible the degradation of refugee women in the cyber realm.

At the same time, terrorist organisations and non-state actors use cyber technology as a propaganda tool to promote their agendas. Cyberspace contributes to the growing anonymity of the online communications network and it is for this reason that terrorist organisations can substantially enlarge their pool of recruits, particularly young people, by exploiting their anti-establishment sentiments.[42] Terrorist organisations such as the so-called Islamic State (IS) have agendas that are particularly harmful to women and possess the cyber knowledge to recruit more followers in the conflict region and elsewhere to their ideology. Thus it is necessary for women to have access to ICT and know how to use it in order to advance gender equality in the region and combat the narrative of violence.

2.2.3 The digital gender gap and capacity-building

Many individuals, particularly the world's poorest, are denied access to the Internet by a combination of high costs and the limited availability of the necessary technology. By and large, women have lower earnings and often have less control over spending than men, and can thus be disproportionately affected by the problem of affordability. A recent study found that women globally have 84 per cent of the level of access to the Internet and mobile phones that is currently enjoyed by men.[43] The Internet gender gap in developing countries, particularly in the Middle East, constitutes a major issue that must be addressed.

Little comprehensive data existed on women's access to the Internet until a report published in 2012 revealed the state of affairs through a study commissioned by Intel Corporation.[44] The study surveyed 2,200 women in developing countries, interviewed experts, and undertook a review of existing literature. It found that 23 per cent fewer women than men are online in developing countries.[45] In some regions the size of the gap can exceed 40 per cent and in many regions the Internet gender gap reinforces sexual inequality.[46] Additionally, when the numbers are added up they show that 200 million fewer women than men were online at the time when the study was conducted.[47] In the report, UN Women states that it is committed to actively working with partners to develop "normative frameworks, policies, and on-the-ground initiatives that build on data and evidence … to promote more holistic solutions".[48] It goes on to say that in order for the gender gap to be bridged, there needs to be an

> improvement to women's access to the Internet and broad range of ICTs, an empowerment of women through digital literacy training and skills building, promotion of the development of gender-sensitive applications that monitor violence against women in partnership with the private sector and civil society, a public service that takes into account the specific needs of women and their surroundings, and the promotion of a digital entrepreneurship among women that fosters social innovation.[49]

This was be achieved through a global marketing campaign whose aim was to get women in developing countries online and was to be led by a coalition of partners who represented different faces of the Internet.[50] These marketing activities were to be combined with efforts to offer women digital and informational literacy training to address ability-related barriers. One example of a coalition that works on the issue of the Internet gender gap is the "Girls in ICT" portal, a partnership between the International Telecommunication Union and WITNER Global Network Women in ICT. This initiative aims at increasing the number of women taking up careers in IT by holding global events such as "Girls in ICT Day", marketing and research.[51]

Addressing the Internet gender gap in the region will result in an improvement in the individual security of women in the Middle East. These women can then have the tools necessary to not only compete in the rapidly evolving ICT job market, but to fight against the narrative of violence in the region and the gender stereotypes that continue to limit progress by using their knowledge to build strong social media platforms that promote gender equality and peaceful practices.

2.3 Cybercrime

2.3.1 The Internet of Things and its impact

The expansion of the Internet of Things[52] into all parts of everyday life is matched by the extraordinary accumulation of private information and increased government information monitoring. Both have a negative effect on users' privacy and offer startling new avenues for criminally motivated ruptures in digital security and even the likelihood of cyberwarfare, including assaults on civilian infrastructure.[53] Malicious actions in cyberspace take many forms; e.g. cyber fraud, cybercrime, spying, and politically motivated attacks. It is important that civil society and state actors understand that not all vindictive cyber actions constitute cyberwar. Cyberwar is more accurately described as the use of force to cause damage or destruction for a political purpose by states or political groups.[54] A cyberattack would be an individual act that is meant to cause damage or fatalities. Cyberwarfare could involve the disruption of essential network content and records, harm to crucial infrastructure, and the advent of uncertainty and suspicion among political leaders.[55]

Cyber threats have been increasing in the region and this is in part due to the fact that the Middle East does not have highly developed organisational structures in place to combat them.[56] Without these structures, it is difficult to carry out investigations requiring complex technical and legal expert knowledge.[57] There is a need for more collaboration among many actors to tackle cybercrime in the Middle East. At present computer emergency response teams and law enforcement agencies in the region work on their own in fighting cybercrime.[58]

2.3.2 State involvement and the scope of cyberwarfare

State-sponsored attacks have objectives aligned with political, social or military interests in the country that conducts them. One example was an attack directed against Iran's nuclear programme in June 2009 using a computer virus known as Stuxnet. Allegedly, both a regional and a Western cyber intelligence agency orchestrated the attack.[59] Stuxnet targeted the computer system controlling the uranium enrichment process of Iran's nuclear programme at Natanz, a heavily secured and underground desert facility. The virus was designed to damage the cascades of centrifuges used to enrich uranium.[60] Despite some disruption to Iran's enrichment capacity, the country actually increased its monthly output of enriched uranium after the attack, according to the International Atomic Energy Agency.[61] There was another attack on Iran's nuclear facilities known as Operation Olympic Games. The attacks on Iranian industrial control systems resulted in centrifuges spinning at speeds that compromised the enrichment process.[62]

Besides Stuxnet and Operation Olympic Games, Iran and other countries have been the targets of other advanced cyber-espionage attacks that have worried security experts, such as Duqu, Flame and Gauss. Gauss targeted financial institutions, the majority of which were in Lebanon, while Flame was a cyber-espionage tool that targeted universities and private industries in Iran, Syria, Lebanon and Saudi Arabia.[63] These tools have the capability of recording audio and keyboard activity by switching on a device's camera or turning an infected telephone into a recording device. During the Flame attack the hackers were able to record Skype conversations and use an infected computer's Bluetooth connectivity to extract information from other Bluetooth-enabled devices nearby, sending the data back to several command-and-control servers around the world.[64]

Analysts have suggested that attacks like Flame are most likely funded by governments, because the attackers have to find vulnerabilities in a computer's operating system that have not been exploited previously, and this requires a substantial investment of money and time. Other, less sophisticated attacks have targeted the Middle East. The 2012 "Mahdi" campaign that infected targets in the region introduced malware into MS Word documents, MS PowerPoint presentations and PDF files.[65] The Mahdi malware adversely affected a wide variety of engineering and financial companies, governments, and academia throughout the Middle East while using simple methods and tailoring them to target specific victims.[66]

2.3.3 Regulatory and preparedness schemes

As a result of such cyberattacks Middle East countries have begun to identify cybersecurity as a major concern among large organisations in the region, and large oil and gas utilities and banks have been strengthening their cybersecurity capabilities. Many Middle East countries have begun to update their cybersecurity capabilities to ensure the safety of their national information infrastructure. The increase in risk of advanced malware is the main catalyst for

the increased demand for cybersecurity in the region. Factors such as the need for unified cyber solutions, strict compliance and data discourse mandates, the risks associated with the maintenance of sensitive data, enhanced enterprise mobility, and the growing spending on security forums are increasing the demand for cybersecurity in the Middle East.

A number of countries, including the UAE, Oman and Morocco, have passed new laws aimed at protecting electronic transactions and prosecuting cybercrimes, while others have vested responsibility for cybersecurity in existing agencies or directorates and have established critical information infrastructure protection policies and cybersecurity plans. Additionally, other countries, such as Jordan, Algeria, and Saudi Arabia, have initiated national incident response protocols and have begun to build cybersecurity awareness and capabilities. While these steps are constructive, they are not sufficient to manage the risks associated with the digital assets and private information of an entire country.

2.4 Cyberterrorism, nuclear security and critical infrastructure

Cyberterrorism is a highly contested term and, as such, some scholars opt to use a narrow definition that focuses on attacks by well-known terrorist organisations against information systems for the purpose of engendering insecurity in society. It can also involve the intentional utilisation of cyberspace, networks and the Internet to cause harm for personal objectives that can be political or ideological. In the past, cyberterrorism appeared to be an abstract concept, but it is now proving to be a real security issue. The world is in a post-modern and post-technology era in which countries are vulnerable to having their ideas, people and infrastructure compromised.[67] Non-state actors have access to a free market that allows the trading of cybernetic weapons and knowledge for facilitating attacks. With this open world, the possibility of a carefully orchestrated attack is much more real. Terrorist organisations are able to send their recruits and students to computer science courses to train them in organising cyberterrorist attacks. Non-state actors, terrorist organisations, and criminals are using cyberspace for their own purposes, and derive benefits from a field that allows individual players to exercise an influence that is disproportionate to their size. IS may pose a more serious threat than any other terrorist group because of its utilisation of modern technology, mastery of online propaganda, and appeal to young, computer-literate individuals. This asymmetrical advantage creates risks that did not attract action among the major powers in the past.[68]

Experts in the field are not yet able to predict the collateral damage for all cyberattacks categorically as a target set moves from tactical, as in the case of deployed military forces, to strategic, as in the case of civilian infrastructure.[69] In the example of attacks that incapacitate networks, damage could be done not only to the target, but also to non-combatants or even the attacker.[70] This makes the risk of unintended consequences difficult to predict. While it is important to note that currently cyberattacks are not as destructive compared to strategic

weapons in the sense that they are unlikely to produce large numbers of physical casualties, these attacks have the potential to target critical infrastructure in a way that negatively affects people's lives. For example, an attack on a hospital could cause casualties by tampering with data, changing prescriptions, or turning off life-support or other critical systems.[71] Kaspersky Lab CEO Eugene Kaspersky touched on the security threat that cyberattacks pose to civilians when he warned that malware threats are becoming more sophisticated because criminals and terrorists are beginning to employ experienced hackers.[72] He claims that both global and regional threats to security are growing, and that globally the key area of vulnerability is "energy in the form of power plants and grids".[73]

2.4.1 Cyberattacks on energy installations, and financial and transport infrastructure

If there is no power, then nothing can work in a country, and this would have devastating consequences. Financial services and transportation could also be attacked, as has happened recently in the region. In terms of regional threats, the Middle East is dependent on the oil and gas sectors, and thus attacks on these sectors would be extremely harmful to the economy and national security.[74]

While there has not yet been a significant case of cyberterrorism, it is essential that all the actors involved understand that as the Internet becomes more pervasive in all sectors of society, individuals and terrorist organisations can use the anonymity afforded by cyberspace to threaten citizens, specific groups, communities and entire countries without the inherent threat of capture or harm to the attacker that other forms of attack would bring. Terrorists will soon have the ability to target the vulnerabilities in ICTs in a way that causes serious harm to civilians.

2.4.2 Cybersecurity and nuclear security

Cybersecurity is directly connected to nuclear security. The Nuclear Security Summit in Washington, DC in March 2016 recognised the growing importance of the security of information, including information held on computer systems, related to nuclear material and technology.[75] Nuclear technology and the knowledge to build these weapons is no longer a monopoly controlled by states, and terrorists are now more than ever able to exploit the cyber vulnerabilities of both nuclear weapons systems and nuclear power installations used for peaceful purposes.

A cyberattack on nuclear weapons systems could potentially occur in the form of attacks on nuclear command and control systems; communication links; weapons and delivery systems; and the computers, hardware and software used to manage and operate nuclear forces; and through attempts to provide false or misleading information to these systems and decision-makers, otherwise known as spoofing. The need for improvements to be made to nuclear security conditions becomes more urgent if one accepts that cyber threats can influence

both precision strike and nuclear weapons, thus affecting both nuclear deterrence efforts and arms race stability.

In terms of both nuclear weapons security and the security of peaceful nuclear installations, the 2016 Nuclear Threat Initiative (NTI) Nuclear Security Index revealed that

> of the 24 states with weapon-usable nuclear materials and the 23 states that have nuclear facilities, but no weapons-usable nuclear materials, 13 received a maximum score for cyber security, but 20 states scored zero and do not even have basic requirements to protect nuclear facilities from cyber attacks.[76]

Furthermore, the NTI reveals that while the Nuclear Security Summit has had a positive effect, an effective global nuclear security system is yet to be put in place.[77] The index finds that many countries are failing to protect their populations; for instance, nearly half of the 45 countries surveyed do not have a single requirement in place to protect their nuclear facilities from hackers.[78]

The NTI index includes a sabotage ranking that focuses on countries with one or more of the following facilities: currently operating nuclear reactors; nuclear power reactors shut down within the last five years; research reactors with a capacity of two megawatts or greater; reprocessing facilities; and spent fuel pools (only if the fuel had been discharged within the last five years and was not associated with a reactor that was still in operation).[79] An act of sabotage could mean a scenario where the targeted nuclear facility releases radiation in a similar way to the Fukushima Daiichi nuclear power plant in Japan in 2011 after a tsunami struck the facility; however, in a case of sabotage the radiation leak would be caused not by a natural event or human error, but an intentional cyberattack. The number of countries that are considering the use of peaceful nuclear energy is growing, but without proper precautions the threat of intentional sabotage by non-state actors is also increasing.

2.4.3 NTI Index sabotage rankings

Three countries from the Middle East and North African region – Egypt, Algeria and Morocco – are referred to in the NTI report.

The index indicates that Egypt ranks near the bottom of the vulnerability to sabotage ranking (43rd of the 45 countries rated). It stresses that the country's nuclear security situation could be improved by introducing stronger laws and regulations for onsite physical protection systems, putting effective response capabilities in place, addressing the insider threat, and having a cybersecurity system at nuclear facilities.[80] Algeria was 42nd in the sabotage ranking out of the 45 countries rated and its conditions could similarly be improved by implementing strong laws and regulations for addressing the insider threat, improving emergency response systems, and ensuring better cybersecurity.[81] Morocco was 40th in the sabotage ranking with

the possibility of improving its nuclear security conditions through considering

> potential levels of radiological consequences of sabotage when designing protection measures, additional controls and limits to access to vital areas, measures to mitigate the insider threat, training of law enforcement to respond to security incidents at nuclear facilities … and improved cyber security requirements at nuclear facilities.[82]

However, these conditions are not unique to these three countries, and the index shows that countries with new or emerging nuclear energy programmes are struggling to deal with the threat of sabotage. These countries should be encouraged to protect their citizens by hosting international peer reviews, increasing their engagement in international initiatives, publishing annual reports, and drawing up and applying nuclear-security-related regulations.[83]

3. Middle East cybersecurity initiatives

Every state in the Middle East is working to defend itself against cyberattack, and some are even creating the capacity to carry out cyber offensives as a pre-emptive means of defence.

3.1 Cyber surveillance of non-state actors

Israel is a good example of a cyber-defence trend with its expansion of Unit 8200, which is responsible for collecting signal intelligence and code decryption.[84] The country set up the National Cyber Bureau in 2010 to coordinate the development of cyber defences. However, cyber defence may also involve cyber offensives. It was publicly acknowledged that Israel was taking proactive steps against Iran and other strategic targets aimed at neutralising both their actual and potential offensive ability. Israel is not alone in this trend: in 2013 the UN Institute for Disarmament Research (UNIDIR) analysed the national cybersecurity programmes worldwide and found that there were 114 such programmes at the time, with 47 of these countries giving some role to the military.[85]

Iran is also building its cyber forces through a programme that is estimated to cost more than US$1 billion. The programme is run by the elite Revolutionary Guards Corps and has recruited a core body of Internet users. Iran is under pressure to form a stronger cyber programme, given that it has been affected by international sanctions. Although Iran's cyber programme is considered to be less advanced than those of the United States, Israel, Britain, China and Russia, Tehran's programmes are growing in sophistication.

Many Middle East countries have cyber surveillance programmes and units that are in the early stages of development. For example, there are reports of a cyber group in Egypt that claims it has attacked the online propaganda of terrorists and that it aims to defend critical Egyptian infrastructure from all terrorist attacks.[87] This is a particularly interesting case because the group aims to confront non-state actors; such actors are a major source of instability in the Middle East, constituting security challenges that have previously only been seen among state actors.[88]

Another cyber unit that was created through a need to defend its government is the Syrian Electronic Army (SEA). This group was created after the start of the civil war in Syria and is composed of Internet hackers who support the Assad regime. They specifically target Syrian opposition groups, using attacks such as denial of services and information, as well as breaking into websites and altering the content.[89] The group has successfully targeted both Syrian opposition and global websites. The organisation was able to hack over 120 websites such as those of the *Financial Times*, *The Telegraph*, the *Washington Post* and *al-Arabiya.*[90] Perhaps the most effective attack was when the SEA broke into the Associated Press's Twitter account and wrote a fake tweet saying that the White House had been bombed and the US president had been injured in the attack. This resulted in a steep drop in the US financial markets and the Dow Jones Industrial Average for several minutes.[91]

3.2 Cyber legislation

Legislation is an integral part of the fight against the global cyber threat. Cyber legislation in the Middle East is either at an early stage or under active development in the majority of states. Legislators in the region deal with cybercrime issues by applying normal jurisdictional measures that often include criminal, regulatory and civil law. However, it may be more effective to tailor legislation specifically to deal with cybercrime.

Jordan, Oman, Saudi Arabia, and the UAE have all taken critical steps in either enacting cybercrime law or introducing special systems.[92] The UAE's Federal Decree Law no. 5, entitled On Combating Cybercrimes, was issued in 2012. The law states that if any individual uses a computer network or electronic information system, such as social media, for the invasion of privacy of another individual or for the "deliberate expression against any person or entity deemed by an ordinary person as insulting or [as an] afflict[ion] to the dignity or honor of that person" they can be "punished through imprisonment of a period of at least six months or through a fine".[93]

Saudi Arabia also has a cybercrime law issued by a royal decree in 2007. It aims to combat cybercrime by identifying crimes and determining punishments to protect "information security, protection of rights pertaining to the legitimate use of computers and information networks, protection of public interest, morals and protection of the national economy".[94] In addition, the Saudi Ministry of the Interior and Communications and the Information Technology Commission can severely punish cybercrimes such as "identity theft, defamation, electronic piracy, email theft, and other unlawful acts".[95]

Oman issued a law to combat cybercrime in 2011. It identifies a wide array of illegal activities, defines each form of cybercrime, and prescribes penalties that range from a fine to imprisonment, depending on the severity of the offence.[96] Jordan has an Information Systems and Cybercrime Law that contains 18 articles dealing with the complete spectrum of cybercrime, including everything from minor offences such as unauthorised access to computer material to more serious crimes like identity theft and credit card fraud.[97]

Furthermore, some countries in the Middle East are beginning to appreciate the importance of safeguarding individuals' personal information and are addressing this through effective data protection legislation. Egypt, Israel, Saudi Arabia and the UAE all have data protection legislation.[98] As an example of how this operates, let us take the cases of two countries, Egypt and the UAE.

3.2.1 Data protection legislation: Egypt

While Egypt does not yet have comprehensive laws that regulate the protection of personal data, it does have piecemeal provisions that deal with data protection in various laws and

regulations already in place. In addition, a comprehensive draft law has been passed by the Egyptian Parliament for combating cyber threats. The Egyptian Constitution contains principles regarding people's rights to privacy, as well as general principles on "compensation for unlawful acts under the Egyptian Civil Code which governs the collection, use, and processing of personal data". There are other laws that provide for the protection and privacy of certain data, such as the Labour Law no. 12/2003, which covers the confidentiality of employees' files containing personal information, and the Banking Law no. 88/2003, which protects the confidentiality of client and account information. Furthermore, the Civil Status Law no. 143/1994 provides for the confidentiality of a citizen's civil status data and the Executive Regulations of Mortgage Finance Law no. 144/2001 covers the confidentiality of the data of mortgage finance companies' clients. The Telecommunications Law no. 10/2003 protects the privacy of telecommunications and imposes penalties ranging from fines to imprisonment. Additionally, Article 57 of the Egyptian Constitution provides for the protection of the privacy and secrecy of, among other things, e-mails, telephone calls and other means of communication. The Constitution could further strengthen its legislation by defining what constitutes data protection and other significant terms such as 'personal data' and 'sensitive personal data'.

It would also be beneficial to create a national data protection authority responsible for data protection in Egypt, employ data protection officers, create specific provisions that regulate online privacy, and have mandatory legal requirements to report data security breaches or losses to the authorities or to data subjects. However, Egyptian law does cover the collection and processing of data. The collection, use or processing of personal data is prohibited if it violates the individual right to privacy according to the principles of the Egyptian Civil Code. The judiciary defines a violation as an act or omission "that violates an obligation imposed by the law or the assumed caution and care of the average man". Data that is considered essential to the data subject's private life requires the consent of the individual before it can be collected or communicated to others, and a competent court will determine whether "specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumes the caution and care of the average man".

3.2.2 Data protection legislation: UAE

In the UAE, legislation in the UAE-Dubai International Financial Centre (UAE-DIFC) has laid down definitions for 'personal data', 'identifiable natural persons', and 'sensitive personal data', and it has a national data protection authority and enforcement capability. The UAE-DIFC defines an identifiable natural person as a "natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, psychological, mental, economic, cultural or social identity" and defines personal data as "any data referring to an identifiable

natural person". The definition of sensitive personal data is any personal data that reveals or concerns "racial or ethnic origin, communal origin, political affiliation or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life". This type of data makes up an individual's identity; thus it is important to define these terms in order for citizens to understand exactly what these laws are protecting. In addition, the UAE-DIFC has a Commissioner of Data Protection, who serves as the national data protection authority in the region.

However, there are problems in that the UAE-DIFC and the rest of the UAE have a different set of cyber-related laws and principles. For example, there is no national data protection authority in the UAE and the concept of "personal data" is defined differently outside the UAE-DIFC. There are also no specific provisions under UAE federal law relating to the type of measures that should be taken or "level of security to have in place against the unauthorized disclosure of personal data". UAE federal law focuses on cybercrime law through offences related to accessing data without permission and/or illegally, whereas it should put security measures in place to deal with both the unlawful use and accidental disclosure of personal data. Current laws focus on reactive rather than proactive security measures. This is done to minimise the risk of liability arising out of a claim for breach of privacy made by a data subject.

On the other hand, the UAE-DIFC law focuses on the security of the individual, which is demonstrated through Article 16 of the Data Protection Law, which states that data controllers must implement

> appropriate technical and organizational measures to protect personal data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing, in particular where sensitive personal data is being processed or where the personal data is being transferred out of the DIFC.

The inconsistency between federal UAE data protection legislation and UAE-DIFC legislation reflects different priorities and responsibilities towards citizens, and this is a conflict of interest that would be worth analysing and removing.

The legislation available in these countries provide a solid framework for data protection, but more needs to be done in light of the scope and frequency of cyber threats and attacks in the region. Countries in the Middle East ought to collaborate with one another to draft regional cyber laws that are in accordance with existing international humanitarian law and their own cultural traditions.

4. The way forward: a multilateral sustainable solution

Cybersecurity in the region is connected to several issues such as socio-economic challenges, regional and transnational terrorism, low levels of cyber education and capability, and the need for stronger regional legislation on the use of cyber technologies. An analysis of these challenges indicates that the most effective response to the Middle East's overarching cybersecurity challenge is through a collaborative approach with input from all key stakeholders. Through an examination of the threat that cyberattacks pose to both national and individual security, it can be said that there are four ways to address the problem of cyber threats: capacity-building, diplomacy, legislation, and the establishment and implementation of appropriate norms. These are discussed in greater detail below.

4.1 Capacity-building

A cybersecurity programme should contain both proactive and reactive capabilities. Most countries in the Middle East focus on the issue of cybersecurity in reactive terms. However, it is also important for states to develop proactive capabilities to address this persistent threat, e.g. by developing information assurance standards that are designed to increase the resilience of a country's critical cyber assets and reduce corresponding risk levels.

This should involve the regular testing of national cybersecurity capabilities to identify exploitable weaknesses and develop mitigation plans, while promoting cybersecurity as a component in the decision-making and daily activities of the state, the private sector, and citizens.[99] Capacity-building is of vital importance to an effective cooperative global effort to secure ICTs and their use.[100] A practical way to promote capacity-building is through training programmes, because it is crucial that the Middle East's leaders, judges, lawyers and law enforcement officials are properly educated on international developments in the field of public policy as it pertains to cyberspace, ICTs, and cybercrime phenomena and cases.[101]

Extending the issue of cybersecurity from theory to practice, integrating emerging issues and challenges is a prerequisite for a resilient and up-to-date cyber ecosystem that can keep up with the rapid pace of evolution of the global network and the threats it faces. Such activities provide a gateway to numerous opportunities. Universities in the region can offer similar opportunities through executive-level training courses for key decision-makers with the aid of regional centres and organisations.

In addition, the UN Conference on Trade and Development can aid in improving developing countries' cyber capacities: its toolbox on cyber laws covers capacity-building workshops at the national and regional level; the preparation and, when needed, revision of a framework of cyber law; and a cyber law tracker.[102] This could help sharpen the skills of policymakers and lawmakers, and build networks in the Middle East that enable collaboration and the sharing of best practices.

Similarly, the International Telecommunication Union (ITU) can play a critical role in ensuring that there are no gaps in states' abilities to protect their citizens from cyber threats, and would be of assistance to the Middle East. The ITU is composed of member states, the private sector and academia, and is mandated by the World Summit on Information Security Action Line C5 to work with all parties in order to build confidence and trust.[103] The ITU covers a range of issues, including dealing with cyber threats and spam, awareness raising, investigating privacy issues, data management, and managing crises when they occur.[104] In addition, the ITU can provide cyber exercises and computer emergency response teams (CERTs) that are facilitated by UNIDIR and other bodies. And while these cyber exercises and CERTs may not be considered effective confidence-building measures, they encourage countries to collaborate at a technical level and confidence can thus be built.

In terms of reactive capabilities, while each country's cybersecurity programmes ought to plan for worst-case scenarios to ensure effective reaction to and recovery from a cyberattack, managing the daily risks of cyber threats can pave the way for managing high-level risks.[105] Furthermore, focusing only on high-impact risks will over-politicise diplomacy efforts and inhibit states' ability to protect their citizens.

4.2 Diplomacy

The Middle East can further its diplomatic efforts to deal with cyber threats by promoting its Internet Governance Forum (IGF). The creation of this forum was based on paragraph 72 of the Tunis Agenda, the outcome document of the second phase of the World Summit on the Information Society held on 16-18 November 2005. The IGF creates a common understanding of how to maximise Internet opportunities and address any Internet-related risks and challenges that arise.

The UN can also assist in furthering diplomatic relations between stakeholders by holding annual Governmental Group of Experts (GGE) panels that are solely focused on cybersecurity issues in the Middle East. These would promote dialogue on the security of ICTs in their use by the states in the region and would help to develop a common understanding of the application of "international law, norms, rules, and principles of responsible State behavior by all stakeholders".[106] The UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security provides a truly universal and multilateral forum for deliberations and consensus building.

These diplomatic efforts are geared towards safeguarding cyberspace from becoming an arena for a cyber arms race and cyber conflict, and ensuring peaceful uses of the Internet that enable the full realisation of cyber technologies' potential for contributing to social and

economic development. It is through these exchanges that states can begin to reduce the risk of cyberattacks through the application of existing norms and international law relevant to the use of ICTs.

4.3 Legislation

In the context of ICT security, the use of force would encompass the destruction of or cause harm to all layers of a state's ICT infrastructure, whether physical or digital.[107] To counter this threat, legislative frameworks to reinforce cybersecurity protocols at the national level are still under development in the various countries of the Middle East, and this should be done in accordance with international humanitarian law.[108] Like all weapons systems, ICT weapons must be used in compliance with international humanitarian law, especially in times of conflict.

The UN Charter, the laws of armed conflict as laid out in the Geneva Conventions, and the Council of Europe Convention on Cybercrime serve as a general framework to assist nations in developing legislation that addresses cybersecurity threats. In their use of ICTs, states in the Middle East must observe their obligations under Article 2 of the UN Charter to settle international disputes by peaceful means, as well as prohibit the threat or use of force.

States are responsible for ensuring that they are developing these new technologies in compliance with international humanitarian law. Each state is required by Article 36 of Additional Protocol I to the Geneva Conventions to determine whether the use of a "new weapon, means or methods of warfare that it studies, develops, acquires or adopts would, in some or all circumstances, be prohibited by International Law".[109]

Furthermore, the 2013 and 2015 reports of the UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security confirm that international law, in particular the UN Charter, is not only applicable to, but essential for "promoting an open, secure, stable, accessible, and peaceful ICT environment".[110] States' adherence to international law lays the ethical groundwork for their use of ICTs.[111] The UNGGE has emphasised the following principles of the charter and other international law as important to the states' commitments:

> sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat of use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other states.[112]

Furthermore, the panelists at the 2015 GGE meeting emphasised the need to apply established international legal principles to cyberwarfare, including, where applicable, the principles of "humanity, necessity, proportionality and distinction".[113] It has to be mentioned that asserting that international humanitarian law applies to cyberwarfare should in no way encourage states in the Middle East to militarise cyberspace or legitimise cyberwarfare.

4.4 Establishment and implementation of norms

Governments have a complex relationship with the Internet. While they use ICTs to protect both their countries' infrastructure and citizens, they can also exploit the Internet by using it for offensive purposes,[114] which could damage critical infrastructure in the Middle East and the global economy. Cyber insecurity at the regional and global level undermines trust, which is why it is essential to identify a set of norms in terms of which the region can manage its ICT interactions. Norms embody established codes of what "actors should do, or refrain from doing, in certain circumstances".[115] The task of interpreting and identifying norms in cyberspace is particularly challenging, because it is a realm of evolving practices, different values to those that have applied previously, and ambiguous agents.[116] However, these norms can be established through continuous diplomatic exchanges among all stakeholders.

It is integral that policymakers study the current norms that apply to cyberspace and the ways in which states use cyber technologies so that they are able to implement an agreed set of norms that conform to national and international law and help to deter and de-escalate cyberattacks. Trust is an important pillar of any information society, especially in terms of ICTs.

It is of relevance to look at the international cyberspace policy of the European Union (EU) in any discussion of norms. The EU functions according to its own set of laws, norms and core values that are integral to its existence and apply as much in the physical world as they do in cyberspace.[117] The EU asserts that responsibility for a more secure cyberspace lies with everyone at all levels of society, from citizens to governments.[118] The EU would be an important model to look at in terms of norm creation in cyberspace, because its cyber strategy outlines its vision of and principles for applying its core values and fundamental rights in cyberspace.[119] The EU believes that "increased global connectivity should not be accompanied by censorship or mass surveillance".[120] Furthermore, the EU constitutes an important cyberspace resource for the global community, given that it fosters international cooperation on cyberspace issues by collaborating with relevant international partners and organisations, the private sector, and civil society to promote an "open, free, and secure cyberspace".[121]

Enforcement of the agreed norms and legislation can be achieved through the creation of threat neutralisation and cyber law enforcement capabilities that protect citizens, the

private sector and the government from cyberattacks.[122] To facilitate this, it is proposed that a central national cybersecurity body be formed in each Middle East country whose purpose would be to define a national cybersecurity strategy, establish a national dialogue, and build a preventive and reactive national cybersecurity capability in the form of an appropriate agency.[123] This body should be independent and not part of any existing public organisation: its impartiality would be critical in ensuring collaborating among all stakeholders. At the same time, this body should be empowered by high authorities such as a national security council and mandated to coordinate regional activities through regional legislation. Egypt, for example, has an impressive model on which to base other countries' national cybersecurity bodies with its High Council for Cybersecurity. This is a 24-member body that is dedicated to creating a national strategy to help government agencies prevent cyberattacks.[124] It also educates people about the threat of hacking, in particular government agencies.[125]

5. Conclusion

Ensuring cybersecurity is an emerging challenge that interlinks with other political challenges in the Middle East, such as critical socio-economic challenges; regional and transnational terrorism; and education, awareness and capacity-building. Recent cyberattacks in the region have demonstrated the shift in the nature of cybercrime. Individuals, non-state actors, and states that commit cybercrime are becoming more sophisticated and organised in their attacks, which cover a range of areas. They may include financially motivated attacks targeting the private sector, politically motivated attacks aimed at governments, specifically engineered attacks focused on hacking intellectual property, and cyberattacks targeting a specific demographic group such as women. The variety of cyber risks highlights the need to establish a proactive cybersecurity approach at the national level.

Many states in the region have started making efforts to update their cybersecurity capabilities and processes. While states have a primary responsibility to maintain a secure ICT environment, the UN should play a role in promoting dialogue on the security of ICTs in the region and continuing its work on developing common understandings regarding the application of international law and norms. It can assist states in the region to improve the security of their ICT infrastructure, create strategies and a governing framework for cybersecurity, and encourage states to further their work in capacity-building. The Middle East has the potential to contribute to a culture of global cybersecurity that promotes a common understanding of international humanitarian law and norms for the peaceful use of cyber technologies by all state actors.

6. Recommendations

6.1 Promoting cybersecurity competence building at universities

It is crucially important to build competencies in information management and governance and the techniques of cybersecurity into higher education programmes on two levels. The first is the technical level, where students learn the basic techniques of information management and cybersecurity as part of computer studies. The second is the training of managers who may not be computer technicians themselves, but will be responsible for the management of those carrying out technical processes. These managers should increase their understanding of the management of information and above all the principles of information governance to prevent unauthorised access to secure information.

Creating government-supported university programmes

The best way to achieve these aims is to provide courses at the master's or diploma levels supported by government as part of its education programme in higher education. This will give information management and governance and cybersecurity the necessary weight and importance to attract students.

Certifying study programmes

These programmes should be certified by universities at diploma level or as higher degrees at master's level and will be included as modules and special diploma courses in both university postgraduate education and apprenticeship and professional education courses.

Reaping the economic potential of investing in education

The investment in this kind of education will yield both monetary and quality benefits. Graduates of these programmes will be in demand in security firms, governments, corporations and the military. Employment opportunities are therefore likely to increase. At the quality level, universities will train a cadre of professionals able to work at both the technical and managerial levels in ensuring cybersecurity.

6.2 Promoting competence building through professional training

In addition to university training, it is important to consider professional training. This would also occur at two levels: pre-service training and on-the-job training. Both are extremely important, especially because cybersecurity is a rapidly evolving field and therefore updating knowledge is a vital part of building and maintaining competence levels.

State personnel training

The state has a key role to play in cybersecurity training, both in government departments and state-owned or state-run enterprises. This should involve induction courses for relevant personnel supported by in-service training courses for both technical and management personnel. In any organisation the aim should be to build a cadre of technical experts and managers able to work together to identify and counter threats and build defences to stop threats before they materialise.

Collaboration with professional certification bodies

It is important to ensure that both technical and management personnel have the relevant qualifications. This in itself is an important part of maintaining security. Whereas universities have their own degrees and diplomas, corporations and governments need an equivalent range of professional qualifications, which could be offered through professional certification bodies.

Improving the competence of the private sector

As with the state sector, the private sector needs the same levels of professional training and certification, particularly where the private sector acts as sub-contractor responsible for the construction and maintenance of national security infrastructure.

Managerial- and decision-making-level training

As previously pointed out, cybersecurity involves not just a cadre of technicians able to operate security systems and spot weaknesses and faults early on and repair them. It also includes managers who are able to ensure that an organisation's security infrastructure is secure.

This involves supervising who has access to the IT system and means of access, limiting access to specific parts of the system, and ensuring that the entire system is secure and that any breaches – potential or actual – are quickly identified and dealt with by technicians.

Knowledge frameworks, job descriptions and the professionalisation of cybersecurity

All this adds up to the establishment and regular updating of a body of knowledge that cybersecurity professionals should know and be able to use when required. It also involves the establishment of clear job descriptions and responsibilities, with officials reporting to a chief information and security officer at board or government cabinet office level. This knowledge framework can be defined by universities, corporations and governments in collaboration with the relevant professional bodies providing qualifications.

6.3 Updating cybersecurity techniques and capabilities

Many states have already announced plans to upgrade their cybersecurity systems, which is a definite need in the Middle East and North African region. A number of possible initiatives have been discussed in this paper; the main ones are summarised below.

Ensuring that states fulfil their responsibilities under Article 2 of the UN Charter to settle disputes by peaceful means

This involves action through UN agencies to effectively 'police' areas of disagreement and act as mediators or appoint mediators to arbitrate disputes.

Creating a global culture of cybersecurity

Experts have predicted that the 21st century will see the development of cyberwarfare, and we have already seen examples of this in many regions of the world. Creating a culture of cybersecurity means three things. Firstly, it means creating awareness of the dangers inherent in the abuse of cyberspace. Secondly, it means all government and corporate organisations should tighten their information management systems and governance to safeguard information security and prevent or at least immediately identify breaches of the system and attempts to tamper with information, and then repair any damage. Thirdly, it means that cybersecurity needs to become an integral feature of education programmes, ranging from school to university and professional training.

Strengthening cooperation mechanisms with national CERTs

The computer emergency readiness teams (CERTS) that were first introduced in the United States in 1988 now exist in all major states. However, operations at a national level are insufficient. In an age of international cybersecurity incidents, cooperation among CERTs is vital to ensure the efficiency of information sharing about incidents and ways of preventing them, and joint action to deal with cybersecurity incidents when needed.

Providing assistance and training to developing countries to improve security in the use of ICTs

An important role of international development ministries and international organisations is to devote a proportion of aid budgets to help emerging economies develop ICTs to enable them to run systems more efficiently and to monitor and combat cybersecurity risks. Such aid should have two dimensions: the supply of equipment, including hardware and software, and, secondly, the provision of training in this equipment's use and also in information management and governance.

Providing access to technologies and methodologies deemed essential for ICT security

A key issue in cybersecurity is confidentiality regarding resources, security methods and intelligence. A clear distinction needs to be made between what corporate and government security organisations need to keep secret and what can be publicly released, however complex the process of making such a distinction would be. Where essential technologies can be made available, this should be done under the auspices of the UN or other international agencies.

Creating procedures for mutual assistance in responding to incidents

When state actors are the victims of cyberattacks they should be able to obtain assistance from CERTs or international agencies that are qualified and prepared to take rapid action to resolve cybersecurity crises or confront threats.

Facilitating cross-border cooperation

At present there is little cooperation among states on cybersecurity due to its sensitive nature. During the World Conference on International Telecommunications in 2012 a number of states requested less control of the Internet, while others demanded greater control. This dichotomy of views poses problems for cross-border cooperation. The Nuclear Security Summit in Washington, DC in 2016 discussed the importance of knowledge and capacity sharing in securing nuclear material and nuclear technology from the threat of cyberattacks. Cross-border cooperation in the Middle East could be facilitated under the auspices of UN agencies and Arab regional organisations.

Developing strategies for sustainable ICT security capacity-building efforts

Because cybersecurity incidents are predicted to increase both in scale and complexity, affecting not just national utilities and financial institutions, but even the political institutions of nation-states, it is important to have more than tactical response units qualified to identify and resolve cybersecurity incidents. Nation-states need to evolve a strategy to build cybersecurity installations, train both technical and administrative personnel, and build a culture of vigilance and caution to ensure that information does not get into the wrong hands.

Arab regional organisations are committed to capacity-building and the sharing of knowledge and technology with the aim of creating a resilient cybersecurity ecosystem, shortening response time in the event of cyberattacks and mitigating the effects of such attacks. The Connect Arab Summit in Doha, Qatar, in 2012 promoted regional initiatives on access to broadband networks, digital broadcasting, open source software, digital content and cybersecurity. Joint follow-up by Arab states, regional organisations and the ITU explored ways of furthering the implementation of regional projects.

6.4 Promoting a culture of cybersecurity

A vital component of global security is cooperation and the willingness to exchange information, assist one another, prosecute terrorist and criminals attacks on ICT, and implement cooperative measures to address threats in compliance with national and international law. This involves providing access to ICT security technologies, creating procedures for responding to incidents, facilitating cross-border cooperation through international and regional agreements, and developing sustainable security capacity-building programmes.

Prioritising ICT security awareness and capacity-building in national plans and budgets

Provision for training in security awareness and equipment upgrades needs to be made in national and regional budgets. This needs to be discussed and agreed at cabinet level with the responsible departments clearly designated, and budgets agreed and distributed by the finance ministry. This budgetary provision can only be effectively initiated at top levels of government and implemented as part of ministerial briefs with specialist civil servants in key positions to ensure proper day-to-day management.

Developing training programmes to help overcome the digital divide

A key issue in international cybersecurity is the digital divide, which is not just a matter of training, but of access. Internet web statistics indicate that the key problem is lack of access to ICTs. This is due to a number of infrastructure issues such as lack of telephone lines and poor reception, and also personal education such as poor literacy skills. Although this is not such an issue at central government level, regional outposts may not have the same resources and personnel. It is most important to pay as much attention to regional ICT access and training within states as to training in central government installations.

The UNGGE also has a role to play in developing training programmes and helping emerging economies to cope with international developments in the field of public policy. The UN Institute for Training and Research could also play an important part in developing training programmes.

Building regional and international cooperation and coordination by creating and strengthening incident response capabilities

An important aspect of creating a global culture of cybersecurity is ensuring that states fulfil their responsibilities under Article 2 of the UN Charter to settle disputes by peaceful means. This would involve relevant UN agencies working closely with national and international CERTS and providing assistance in developing technical skills and

appropriate legislation, strategies, and regulatory frameworks to allow Middle East governments to fulfil their responsibilities and bridge the divide in the security of ICTs and their use. One of the most ways of utilising UN resources is through the UNGGE. Individual states can use this agency to raise international awareness of their concerns regarding cybersecurity.

At a strategic level the work of the ITU and the Organisation for Economic Cooperation and Development has been important in creating programmes for cybersecurity competence and capacity, but more needs to be done. To take the Middle East as an example, the lack of infrastructure and cybersecurity capacity has increased the risk of cyberattacks, especially the risk of terrorist groups mounting cyberattacks on governments and nuclear power installations. Cooperation among state institutions across the region under the auspices of the UN is essential to the success of training and capacity-building. The need for a jointly developed and effective cybersecurity strategy is paramount.

Creating a stronger international legal framework to control cybersecurity

At the moment international courts of justice have no authority to intervene or rule on issues of cybersecurity – and, indeed, in many cases lack the expertise to do so. The key legislative instrument is Article 2 of the UN Charter, although this is not adhered to, especially in the area of cybersecurity disputes. The UN legal framework needs to be strengthened, as does the international authority of CERTs to intervene whenever cybersecurity disputes arise and negotiate settlements. The UNGGE has a key role to play in supporting legal, technical, and policy initiatives for cooperation at the regional and multilateral levels to foster common understanding of cybersecurity threats. It is important that this initiative should not be limited to governments, but also extends to the private sector, academia and civil society organisations.

Finally, the UN itself can play a leading role in promoting dialogue on the application of international law and norms, rules, and principles for responsible action to deal with cybersecurity threats. In 2016 the UN General Assembly agreed to consider convening a new GGE on Developments in the Field of Information and Telecommunications.

Endnotes

1 W. Tohme et al., *Cyber Security in the Middle East: A Strategic Approach to Protecting National Digital Assets and Infrastructure*, Strategy&, 27 March 2015, http://www.strategyand.pwc.com/reports/cyber-security-middle-east

2 Internet World Stats, "Internet World Stats Usage and Population Statistics Africa", 2016, http://www.internetworldstats.com/africa.htm

3 GCIC (Global Commission on Internet Governance), *One Internet*, Centre for International Governance Innovation and Chatham House, 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-06-21-global-commission-internet-governance.pdf

4 Ibid.

5 Ibid.

6 Intel Security and Centre for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, 2014, https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

7 R. Cressey and M. Nayfeh, *Cyber Capability in the Middle East: Seizing Opportunity while Managing Risk in the Digital Age*, 2012, http://www.booz.dk/content/dam/boozallen/media/file/cyber-capability-in-the-middle-east-vwpt.pdf

8 M.N. El-Guindy, *Middle East Cyber Security Threat Report 2014*, December 2013, http://www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014

9 A. Blom et al., *Cyber Security and Data Protection in the Middle East*, Financier Worldwide, November 2013, https://www.financierworldwide.com/cyber-security-and-data-protection-in-the-middle-east/

10 Ibid.

11 El-Guindy, *Middle East Cyber Security Threat Report 2014*

12 Ibid.

13 A. Ünver and G. Kim, "Cross-border Data Transfers and Data Localization", EDAM Cyber Policy Paper Series no. 2016/3, 2016, http://www.edam.org.tr/en/File?id=3192

14 Ibid.

15 Ibid.

16 Ibid.

17 S. Hashem, International Telecommunications Union (ITU) Interviews at the Global Symposium for Regulators 2016 (GSR16), 2016, https://www.youtube.com/watch?v=eftNdYsa0iE

18 Ibid.

19 Intel Security and Centre for Strategic and International Studies, *Net Losses*.

20 J. Tebbs, *Adjusting the Lens on the Economic Crime in the Arab World*, PwC, 2016, http://www.pwc.com/m1/en/publications/documents/economic-crime-in-the-arab-world-2016.pdf

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Ibid.

28 Ibid.

29 Ibid.

30 Ibid.

31 GCIC, *One Internet*.

32 Ibid.

33 Ibid.

34 M.N. El-Guindy, *Cybercrime Challenges in the Middle East*, 13 October 2012, http://www.issa-eg.org/res/Cyber-Sec-Energy-Cybercrime-elguindy.pdf

35 UN Women, "A Snapshot of UN Women's Work in Response to the Crisis in Syria", 3 May 2016, http://www.unwomen.org/en/news/stories/2016/2/a-snapshot-of-un-womens-work-in-response-to-the-crisis-in-syria

36 UN Broadband Commission for Digital Development, *Cyber Violence against Women and Girls: A World-wide Wake-up Call*, 2015, http://www2.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender report.pdf?v=1&d=20150924T154259

37 Ibid.

38 Ibid.

39 FIDH (International Federation for Human Rights), *Violence against Women in Syria: Breaking the Silence*, December 2012, https://www.fidh.org/IMG/pdf/syria_sexual_violence-web.pdf

40 Ibid.

41 Ibid.

42 G. Sibioni et al., "The Threat of Terrorist Organizations in Cyber Space", *Military and Strategic Affairs*, Vol.5(3), 2013.

43 GCIC, *One Internet*.

44 Intel Corporation, *Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-income Countries*, 2012, http://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

45 Ibid.

46 Ibid.

47 Ibid.

48 Ibid.

49 UN Broadband Commission for Digital Development, *Cyber Violence against Women and Girls*.

50 Intel Corporation, *Women and the Web*.

51 Ibid.

52 The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

53 GCIC, *One Internet*.

54 J.A. Lewis, "Thresholds for Cyberwar", Center for Strategic and International Studies, 1 October 2010, https://www.csis.org/analysis/thresholds-cyberwar

55 Ibid.

56 El-Guindy, *Cybercrime Challenges in the Middle East*.

57 Ibid.

58 Ibid.

59 E. Blanche, "Cyber Wars", *The Middle East*, Vol.38(12), December 2012. See also E. Nakashima and J. Warrick, "Stuxnet was Work of U.S. and Israeli Experts, Officials Say", *Washington Post*, 2 June 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

60 Blanche, "Cyber Wars".

61 J. Warrick, "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack," *Washington Post*, 15 February 2011, https://www.washingtonpost.com/world/irans-natanz-nuclear-facility-recovered-quickly-from-stuxnet-cyber-attack/2011/02/15/ABUIkoQ_story.html?utm_term=.149a3acaf9c9

62 D.E. Sanger, "Mutually Assured Cyberdestruction?" *New York Times*, 2 June 2012, http://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html

63 T. Hamid, "Cyber Warfare in the Middle East Is No Game", *The National*, 2012, http://www.thenational.ae/business/industry-insights/technology/cyber-warfare-in-the-middle-east-is-no-game

64 Ibid.

65 K. Geers et al., *World War C: Understanding Nation-state Motives behind Today's Advanced Cyber Attacks*, FireEye, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

66 Ibid.

67 Sibioni et al., "The Threat of Terrorist Organizations in Cyber Space".

68 Ibid.

69 J.A. Lewis, "Cyber Attacks, Real or Imagined, and Cyber War", Center for Strategic and International Studies, 11 July 2011, https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war

70 J.A. Lewis, "Thresholds for Cyberwar", Center for Strategic and International Studies, 1 October 2010, https://www.csis.org/analysis/thresholds-cyberwar

71 Ibid.

72 D. Carroll, "The Threat to the Middle East from Cyber Criminals and Terrorists", Gulf Business, 14 December 2015, http://gulfbusiness.com/the-threat-to-the-middle-east-from-cyber-criminals-and-terrorists/

73 Ibid.

74 Ibid.

75 Nuclear Security Summit, Washington, DC, 2016.

76 NTI (Nuclear Threat Initiative), *The 2016 NTI Nuclear Security Index: Theft and Sabotage*, January 2016, http://www.ntiindex.org/wp-content/uploads/2016/03/NTI_2016-Index-Report_MAR-25-2.pdf

77 Ibid.

78 Ibid.

79 Ibid.

80 Ibid.

81 Ibid.

82 Ibid.

83 Ibid.

84 UNIDIR (UN Institute for Disarmament Research), "The Cyber Index: International Security Trends and Realities", 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

85 UNIDIR, "UNIDIR Cyber Stability Seminar 2015: Regime Coherence", http://www.unidir.org/programmes/emerging-security-issues/annual-cyber-stability-conference/cyber-stability-seminar-2015-regime-coherence

87 J. Vaentino-Deveries and D. Yadron, "Cataloging the World's Cyberforces", *Wall Street Journal*, 11 October 2015, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710

88 G. Siboni, "The Impact of Cyberspace on Asymmetric Conflict in the Middle East", *Georgetown Journal of International Affairs*, 29 April 2015, http://journal.georgetown.edu/the-impact-of-cyberspace-on-asymmetric-conflict-in-the-middle-east/

89 Sibioni et al., "The Threat of Terrorist Organizations in Cyber Space".

90 Ibid.

91 P. Foster, "'Bogus' AP Tweet about Explosion at the White House Wipes Billions off US Markets", *The Telegraph*, 23 April 2013, http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

92 El-Guindy, *Cybercrime Challenges in the Middle East*.

93 UAE (United Arab Emirates), On Combating Cybercrimes: Federal Decree-Law no. 5 of 2012.

94 M.A. Saeed, "Cyber Security and Data Privacy Law in Saudi Arabia", Financier Worldwide, April 2015, http://www.financierworldwide.com/cyber-security-and-data-privacy-law-in-saudi-arabia/#.V2buhed950s

95 Ibid.

96 Oman, Issuing the Cybercrime Law, Royal Decree no. 12, 2011.

97 Jordan, Information Systems and Cybercrime Law, 2010, https://www.unodc.org/res/cld/document/information-systems-crime-law_html/Jordan_Information_Systems_and_Cyber_Crime_Law.pdf

98 Data in the following two sections, 3.2.1 and 3.2.2, derive from this report: DLA Piper, *Data Protection Laws of the World*, 2017, https://www.dlapiperdataprotection.com/system/...dla...data_protection/.../handbook.pdf

99 Tohme et al., *Cyber Security in the Middle East*.

100 S. Aboul-Enein, "Input Paper for the Work of the Group of Governmental Experts", *Proceedings of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 26 July 2015, http://www.gcsp.ch/News-Knowledge/Experts/Fellows/Aboul-Enein-Amb.-Dr-Sameh-Aboul-Enein/Selected-publications

101 Ibid.

102 UNIDIR, "Panel 2: Avoiding Dissonance: A Round Table on Future Inter-Regional Collaboration", *UNIDIR Cyber Stability Seminar 2015: Regime Conference,* Geneva, 2015, http://www.unidir.org/files/publications/pdfs/cyber-stability-seminar-2015-en-636.pdf

103 Ibid.

104 Ibid.

105 Tohme et al., *Cyber Security in the Middle East*.

106 UNGGE (United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

107 Aboul-Enein, "Input Paper".

108 S. Aboul-Enein, "Global Cooperation in Cyber Space: Plenary Panel III on Promoting Measures of Restraint in Cyber Armaments", conference on "Challenges to Cyber Security Development on a Regional Level", Berlin, 4 December 2014, http://www.gcsp.ch/News-Knowledge/Experts/Fellows/Aboul-Enein-Amb.-Dr-Sameh-Aboul-Enein/Selected-publications

109 ICRC (International Committee of the Red Cross and Red Crescent), "International Humanitarian Law and the Challenges of Contemporary Armed Conflict", 32nd International Conference of the Red Cross and Red Crescent, Geneva, 8-10 December 2015, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

110 UNGGE, *2015 UN GGE Annual Report*.

111 Ibid.

112 Ibid.

113 Ibid.

114 UNIDIR, "Panel 2".

115 T. Erskine and M. Carr, *Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace*, NATO CCDCOE Publications, 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch5.pdf

116 Ibid.

117 EU (European Union), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

118 Ibid.

119 Ibid.

120 Ibid.

121 Ibid.

122 Tohme et al., *Cyber Security in the Middle East*.

123 Ibid.

124 CENTCOM (United States Central Command), "A Leader in Regional Cyber Security: Dr. Sherif Hashem", *UNIPATH*, 2017, http://unipath-magazine.com/a-leader-in-regional-cyber-security-dr-sherif-hashem/

125 Ibid.

Geneva Papers Research Series

No.1 – 2011 G. P. Herd, "The Global Puzzle: Order in an Age of Primacy, Power-Shifts and Interdependence", 34 p.

No.2 – 2011 T. Tardy, "Cooperating to Build Peace: The UN-EU Inter-Institutional Complex", 36 p.

No.3 – 2011 M.-M. Ould Mohamedou, "The Rise and Fall of Al Qaeda: Lessons in Post-September 11 Transnational Terrorism", 39 p.

No.4 – 2011 A. Doss, "Great Expectations: UN Peacekeeping, Civilian Protection and the Use of Force", 43 p.

No.5 – 2012 P. Cornell, "Regional and International Energy Security Dynamics: Consequences for NATO's Search for an Energy Security Role", 43 p.

No.6 – 2012 M.-R. Djalili and T. Kellner, "Politique Régionale de l'Iran: Potentialités, Défis et Incertitudes", 40 p.

No.7 – 2012 G. Lindstrom, "Meeting the Cyber Security Challenge", 39 p.

No.8 – 2012 V. Christensen, "Virtuality, Perception and Reality in Myanmar's Democratic Reform", 35 p.

No.9 – 2012 T. Fitschen, "Taking the Rule of Law Seriously", 30 p.

No.10 – 2013 E. Kienle, "The Security Implications of the Arab Spring", 32 p.

No.11 – 2013 N. Melzer, "Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare", 75 p.

No.12 – 2013 A. Guidetti et al., ''World Views: Negotiating the North Korean Nuclear Issue", 47 p.

No.13 – 2013 T. Sisk and M.-M. Ould Mohamedou, "Bringing Back Transitology: Democratisation in the 21st Century", 36 p.

No.14 – 2015 H. J. Roth, "The Dynamics of Regional Cooperation in Southeast Asia", 35 p.

No.15 – 2015 G. Galice, ''Les Empires en Territoires et Réseaux", 42 p.

No.16 – 2015 S. C. P. Hinz, "The Crisis of the Intermediate-range Nuclear Forces Treaty in the Global Context", 36 p.

No.17 – 2015 H. J. Roth, "Culture - An Underrated Element in Security Policy", 40 p.

No.18 – 2016 D. Esfandiary and M. Finaud, "The Iran Nuclear Deal: Distrust and Verify ", 44 p.

No.19 – 2016 Dr. S. Martin, "Spying in a Transparent World: Ethics and Intelligence in the 21st Century", 42 p.

No.20 – 2016 A. Burkhalter, "Définir le Terrorisme: Défis et Pratiques", 50 p.

No.21 – 2017 M. Finaud, "'Humanitarian Disarmament': Powerful New Paradigm or Naive Distopia?", 48 p.

Photo credit
Cover
joffi - Pixabay

Where knowledge meets experience

GCSP - Geneva Centre for Security Policy
Maison de la paix
Chemin Eugene-Rigot 2D
P.O. Box 1295
CH - 1211 Geneva 1
T + 41 22 906 16 00
F + 41 22 906 16 49
info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-100-3