Cyberwarfare – Associated Technologies and Countermeasures

Nishan Chelvachandran, Stefan Kendzierskyj, Yelda Shah, and Hamid Jahankhani

Abstract With the development of automated and AI technology permeating into all sectors of public, private and industry life, the interconnectivity of once remote, siloed and air gapped systems is on the increase. Whilst this affords productive, streamlined and efficient ways of working, monitoring and maximise the effectivity of these systems, it is the connectivity, that can create a critical vulnerability. This vulnerability, is the source of exploitative measures that we refer to in the context of cyberwarfare. Where state and or adversarial threat actors can, utilising mechanisms on the internet, infiltrate, manipulate and attack these systems, to great and potentially devasting effect. It is paramount that the appropriate measures are taken to minimise the risk of these threats and vulnerabilities, through the review and security of internal systems, but also understanding where the vulnerabilities in the systems could lie, and to what effect they would cause should they be exploited. It is also important to understand not only the capabilities of how to respond should such an attack take place, but also the proportionality and legal of such responses.

Keywords Tallin · Cyberwar · Cyberops · SCADA · ICS · Intelligence · Cyberthreat · Attribution · Countermeasures

N. Chelvachandran (✉)
Open Innovation House, Saidot OY, ESPOO, Finland
e-mail: nishan@cyberreu.co.uk

S. Kendzierskyj
Cyfortis, Worcester Park, Surrey, UK
e-mail: stefan@cyfortis.co.uk

Y. Shah · H. Jahankhani
Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-35746-7_2

1 Cyberwar – A New Weapon of Mass Effect

Cyber warfare involves the actions by a nation sate or international organisation to attack and attempt to damage another nation's computer or information networks. Cyber war targets systems that are critical to maintaining a nation's way of life, in part, to cause widespread panic and uncertainty. These systems can include financial systems, energy power grids or plants, healthcare, water, communications systems, transport systems and food and agricultural systems. As Critical National Infrastructure, C4ISR systems, Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) become both more interconnected, and augmented through automation and AI powered decision making processes, cyber security has become one of the main concerns in securing and defending these critical systems. The intrinsic and high impact that these systems play within a Nation's critical national infrastructure, and in the coordination and implementation of public and private sector services, means that these mechanisms are a prime target for adversarial actors, both in the unknown or rogue threat actor context, or in conventional warfare constructs. Cyberwarfare is and further becoming as devastating if not more so, that both conventional weapons and those of mass destruction, whilst, seeming conducted remote, with no risk to life for the threat actor during the action taken. In the example of a SCADA system, for example in a water treatment facility, a remote operator can take control of the system and issue commands to open a value, setting or changing temperature points, stopping pumps, or spoofing sensor readings to affect chemical adjustments for the treatment of the water. Such an attack could prove difficult to initially detect and have a massive impact on a population area of a targeted country or state. A real-world example of such an attack on critical national infrastructure was an attack in December 2015, whereby the Ukraine was affected by a massive power outage after the national electrical grid suffered an attack on one of its SCADA systems. This caused about 230,000 people to not have power for several houses. There have also been reports of attacks on key infrastructure systems of a small dam in New York State and the Wolf Creek Nuclear Operating Corporation. According to a report from the UK's General Communications Headquarters (GCHQ), and the National Cyber Security Centre (NCSC), there are also concerns about suspicious attacks that have occurred on the UK Energy Sectors.

It is observed that much of the critical national infrastructure in western countries, is not solely operated, maintained and managed by public sector agencies, but that the private sector are also key stakeholders in the infrastructure, its operation and maintenance. As such, it is important that the private sector also plays a significant role with public sector agencies to ensure these securities of such infrastructure, and that the risk from the threat landscape is minimised.

Considerations should also be made towards the wider security and governance constructs. Cybersecurity in itself does not solely revolve around network security or the technological layer of these systems, but also the information and governance

frameworks that are in place. The security and management of data and information, to prevent breaches and leaks are just as critical. In most cybersecurity practice, humans are often seen to be the weakest link in information security.

SCADA systems play a large role in critical national infrastructure; however, attention should also be paid to the Internet of Things, or IoT. IoT, while widespread in consumer markets in various products, smart speakers, appliances, toys, it is their sensor functionality that places a key role in infrastructure systems as we see today. For example, in healthcare critical infrastructure, IoT devices and sensors are used in hospitals and clinics, pharmaceutical and testing labs, as well as human interactive devices, such as medical devices and implantable devices. IoT attacks can be classified into three types of attack vectors:

1. Computational capabilities
2. Listening Capabilities
3. Broadcasting Capabilities

With computational capabilities, data modification or impersonation attacks can be launched by an adversary. With listening capabilities, a threat actor can listen and perform eavesdropping or track critical healthcare data within the healthcare infrastructure. And on broadcasting capabilities, a threat actor can replay the critical data from healthcare infrastructure.

Another area of IoT rich implementation is in transportation, but with the development of autonomous transportation, and smart traffic and transportation management. IoT devices have been the backbone for the growth and development of this sector, with technologies utilising both various systems, and data collection and use in a wider network in order to enable the infrastructure. Such technologies include:

- Machine Vision
- In-Vehicle Devices
- Global Positioning System (GPS)
- Acoustic Sensors
- Radar
- Light Detection and ranging
- In-vehicle sensors
- Electronic devices
- Roads/Structures on which the vehicles drive
- Odometrical sensors
- Maps

Each of these strands presents an avenue and potential threat vector for adversaries to target to exploit or influence transportation infrastructure. The manipulation of traffic management systems to cause gridlock and congestion in a major city, whilst superficially could be seen as an inconvenience, can quickly turn into a matter of critical national security, which coupled with attacks on other infrastructure systems, such as electrical or gas grids.

IoT devices are also affected by a number of major security issues:

- Flash network traffic: Sudden High number of end-user devices and new things (IoT).
- Security of radio interfaces: Radio interface encryption keys sent over insecure channels.
- User plane integrity: No cryptographic integrity protection for the user data plane.
- Mandated security in the network: Service-driven constraints on the security architecture leading to the optional use of security measures.
- Roaming security: User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
- Denial of Service (DoS) attacks on the infrastructure: Visible nature of network control elements, and unencrypted control channels.
- Signalling storms: Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
- DoS attacks on end-user devices: No security measures for operating systems, applications, and configuration data on user devices

2 5G as an Enabler

In order for the widespread IoT integrated in infrastructure and wider systems, the devices will not only need to interact with each other and with a base station to response to signals, it requires a faster and stable internet connection, which enables higher data rates for the purpose of information transfers. The development of the 5G protocol, enabling higher data transfer speeds with lower latency means that as 5G begins to roll out across the telecoms infrastructure, there will in turn be a boom in the enabling and utilisation of IoT and automation across sectors and industry. However, exchanging data in terms of transmitting and receiving information via a local network could be feasible but the more complex the amount of information gets, the more data rates it requires. Millimetre wave communication technology is one of the core parts of 5G networks and is expected to offer wireless data transfer by settling for a higher bandwidth. However, the drawback to this technological concept is that the transmission distance of this particular wave is known to be limited into 100 m in the atmosphere. And so, while the line of sight transmission distance degrades quickly compared with previous generations of mobile telecoms protocols, a proposed workaround or solution would be the use of a densification strategy, in that areas utilising 5G technology would have increased radio head, node and relays, to increase the density of the covered area, and so minimise degradation in the signal. However, this requires a great deal of improvement and investment into the mobile telephony infrastructure.

With the implementation of new telephony infrastructure, one of the significant features of 5G to consider, is data handling and storing solutions. The telecoms manufacturer, Huawei points out that *"security"* as such, remains an indispensable factor for business continuity. Furthermore, Huawei suggests the consideration of applying privacy and security properties from former generations of mobile network to the upcoming mobile network (5G) so that business continuity can be provided.

By mitigating the impact of security breaches and understanding the influence that risk factors have, business continuity can be subject to audit through consistent safeguarding. With the 5G network adding function and enhancement to the reliability and availability of faster wireless service to applications, appliances and other 5G driven technologies, the security issue gains importance and further highlight to 5G. 3GPP's newest Release 15, introduces the development for additional space for massive connections between devices but also to deliver faster services with reduced latency. Under section 7.3 of 3GPP's technical specification in Release 15, it is stated that this newest release builds on the LTE features for Machine-Type Communications (MTC) introduced in Release 13 and Release 14 by adding support for new use cases and general improvements with respect to latency, power consumption, spectral efficiency, and access control.

Although, 5G will be capable to cover high numbers of devices, machines and other appliances, the amount of data retrieved and processed will increase enormously.

That is when the confidentiality of vulnerable information may get violated.

Another vulnerability to the 5G network as well as wider critical infrastructure, is the interconnection and dependence on the infrastructure as a whole to be operational as a whole. A crucial point for communications is the power grid. **Power supply** depicts a crucial point when assessing risks, the 5G network has on users and the security structure of a nation. The collapse or disruption of a wired power supply systems might a huge cascade effect on wider systems within the network chain, such as data handling and electrical systems.

Wireless communication systems have been prone to exploitation of security vulnerabilities from their inception. However, with the proliferation of 4G and soon to be 5G networks, the proliferation of smart devices into the mobile domain, with multimedia traffic, and new services with vast quantities of data, have greatly diversified and given huge complexity to the corresponding threat landscape. The dynamic threats that will come from the proliferation of 5G, will also affect the interconnected systems that will rely on 5G. It is crucial to address these issues both in these existing systems, and potential new systems that will be realised with the use of 5G.

A privacy by design approach should be adopting with 5G and it's use, where privacy is considered from the beginning, with features built-in in its implementation. Better mechanisms for accountability, data minimisation, transparency and openness should also be drafted.

3 Cyberthreat Intelligence

In order to appropriately predict, respond and mitigate or minimise the growing threat from Cyberwar, resources and work must be conducted to explore and review the threat intelligence of would-be victim systems. Cyber threat intelligence refers to the intelligence collected before a threat actor attacks a victim system. Organisations and agencies use cyber threat intelligence to mitigate risks relating to cyber-attacks, such as zero-day exploits, internal and external threat actors or Advanced Persistent Threats (APTs). This approach allows for a proactive stance to cybersecurity to be taken and utilise possible countermeasures in advance of an attack. There are multiple sources by which such intelligence can be gathered, such as Open Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), human intelligence (HUMINT), technical intelligence and intelligence from the dark web.

The UK's NCSC classifies Cyberthreat Intelligence into 4 categories:

1. Strategic Cyber Threat Intelligence – This utilises data, high level information and a timely warning of cyber threats, consumed at board or other senior level decision making level. Strategic cyber threat intelligence formulates an overall picture of both the intention and capabilities of threat actors and their impact at a high level.
2. Tactical Cyber Threat Intelligence – This involves data that is obtained from real-time monitoring of systems. This data refers to real time systems events linked to an adversary's actions against a system. This intelligence is used by cyber defensive roles to ensure that their response and investigation systems are prepared for possible tactics used by adversaries.
3. Operation Cyber Threat Intelligence – This involves the fata that gives details about a specific incoming attack. This can include malware, campaigns or cyber weapon tools. The insights gained from this intelligence guides and supports responses to specific incidents, as well as aiding in the assessment of determining future attacks and the organisational ability to do so.
4. Technical Cyber Threat Intelligence – This refers to the data that is consumed through technical means. For example, a suspected malicious IP address of a threat action. This intelligence has a short lifespan, as a threat actor can change their IP change. However, as part of the larger cyber intelligence landscape, technical intelligence helps defensive operators take preventative action, as well as in the investigative reviews post attack.

4 Attribution

The importance of attribution splits the global cybersecurity communities, both in private sectors, influencers and the operating community. In political and traditional legal and warfare frameworks, the attribution of a threat, potential attack or attack

sustained by a victim state by an adversarial nation state is a factor a precursor to a pre-emptive or retaliatory attack against the adversary. Intelligence and other factors also play into responses, however, an adversary or must be known in order to direct a response.

In the cyber landscape however, this is not as straight forward as in a traditional or conventional scenario. The availability and capabilities of cyber weaponry or mechanisms that can be weaponised are not solely available to military or defensive agencies or organisations. Solo operators or lone wolves can be as effective in an attack or response as a nation state operator. By virtue of privacy and other such technological apparatus available, attribution is not as simple as once thought. VPN technology enables a user to encrypt their IP address and traffic through a data tunnel and "appear" to operate from another geographic location. The Dark Web and TOR network also allows users to mirror and redirect their traffic through multiple nodes across the world, making tracing very difficult. Of course, a cyber attack in itself may not necessarily be performed by a real time user. Malware, viruses and botnets can infect and spread across many machines undetected, before opening their payload and becoming operational, instigating coordinated attacked. Attribution in this sense becomes more difficult, as many of the tools, code and software used in the commission and formulation of these "cyber weapons", are available "off the shelf", and available for purchase by a user who may not necessarily have or require the full technical knowledge and capabilities to code such scripts.

There is also the recurring issue of legislation and jurisdiction in this instance, in that, the traffic pertaining to the adversarial attack may have been routed through a nation to give the appearance that they are the perpetrators. Or, if the operator is identified as not being affiliated or acting on behalf of a nation state, then when and where the operator was during the time that the attack was perpetrated needs to be taken into account. The complexity of which legislation applies and in which context, is something that has been discussed in the two published Tallinn Manuals, for Cyberwar and Cyberoperations. These manuals discuss and compile legislation from multiple states, relating to maritime law, international law, legislation relating to surveillance and data protection, as well as security and rules of engagement. Authors of the manual also argued that as cyber warfare increasingly becomes part of and a mechanism utilised in wider conflict, that peacekeeping organisations such as the UN will need to have a cyber defence or peacekeeping capability. However, research into cyber warfare has shown that there is still no answer to what actually constitutes an armed attack in cyber space, and what the ethical boundaries of cyberwarfare are. As such, there currently would be great difficulty for the UN Security Council to agree upon how to enforce peace in a cyber conflict.

A multilateral approach can be used to detect attacks, and potentially perform attribution, as even large intelligence organisations have limited technological and human budgetary capabilities to effectively achieve global coverage.

The existence of the 5-eyes intelligence forum, consisting of the UK, US, Canada, Australia and New Zealand, is one of example of this. This expanded to the 9 eyes forum after the attacks on the US on September 11th, to a wider cooperation

including Denmark, France, the Netherlands and Norway. It has continued to expand, and now is referred to as 14-eyes intelligence cooperation, including Belgium, Italy, Spain, Sweden and Germany.

5 Countermeasures

Under international law, a state is entitled to take countermeasures for breaches of international law against it, that are attributable to another state. Countermeasures are acts by an injured state against another state that would ordinarily be unlawful but are legally justified as responses to the offending state's unlawful activity. The use of countermeasures is subject to strict conditions. The purpose is to encourage the offending state to stop its unlawful activity, rather than to punish. The countermeasures must also be proportionate. And they must not use force.

As discussed in the Tallinn Manual, there is no reason why cyber operations may not in principle be used as a countermeasure in response to a breach of international law. There is nothing in their nature to make an exception for them.

In order to consider countermeasures to cyber-attack, a comprehensive approach to cybersecurity should be taken. The holistic review of internal systems and processes in place, to identify vulnerabilities and making appropriate amendments and adjustments to harden vulnerable systems, is the best way of countering the threat of a cyber-attack. By the virtue of any cyberattack, is the exploitation of vulnerabilities in a system. At a very minimum, internal practices must be conducted to create a minimal base level of security. These can include:

- Continuous Risk Assessment
- IT Environmental Health
- Authentication
- Internal Commitment and responsibility
- Data Retention
- Access to information
- Preventative, detective and Corrective security controls

To further mitigate and harden such internal vulnerabilities, multiple global intelligence agencies agree that the following should also be addressed:

5.1 Education

Employees of an organisation must be aware of the kinds of attacks that can occur and what they should do about them. This includes learning proper operating procedures, the key attack targets, and the classic attack methods. Some studies have shown education to be more effective than any other countermeasure for protecting information systems since knowledge of information-systems security is not a requirement for most jobs.

5.2 Legal Responses

In most western allied states, laws prohibit eavesdropping on communications and damage to computers. But most attackers do not worry about getting caught, since it is hard to track them down and laws are hard to apply. Laws can however be effective against repeat offenders within a given legal jurisdiction, like spies selling secrets.

5.3 Patches

It is important to fix flaws or bugs in software as soon as they are discovered, since attacks are typically launched within days of the discovery of major flaws. Manufacturers provide "patches", "security updates", or "service packs" to fix flaws, in the form of modified software that you must go to their Web site to download. Software that has been sold for a significant period of time generally requires fewer future patches because programmers have had more time to find and fix its flaws.

5.4 Backups

Since many attacks destroy data or programs, making copies of digital information is essential to recovery from attack. Backups need to be done for any critical information and need to be stored some distance from the systems they track so no common disaster affecting both locations is likely. Optical-disk storage is preferable for backups because it cannot be as easily damaged as magnetic media can be. A backup can be an entire duplicate computer system when it is important to maintain continuous operation.

5.5 Access Controls

Automated access controls are important for cyberspace. Access controls for computers are generally managed by passwords that must be supplied to log on and use resources. Controls can be set for individuals or for groups of people, and they can apply separately to reading, writing, or execution of resources, or to the ability to extend those privileges to other users. Access controls for networks are enforced by "firewalls", dedicated computers on a local-area network that restrict traffic to and from the network according to simple rules on such features as origin and communications protocol. Unfortunately, access controls are vulnerable to many attacks mentioned above, and will not generally protect against attacks by insiders like staff.

5.6 Encryption

Encryption hides data in some form that cannot easily be read; you then supply a character-string "key" to decode it when you need it Any attempts to modify encrypted data will result in undecipherability, so you can tell if encrypted messages or programs have been modified. Strong and virtually unbreakable methods of encryption have been developed recently with public-key cryptography. Encryption methods can also be used for authentication or to provide digital signatures on documents to prove who wrote them and when. Encryption has been touted as a solution to many security problems, however, it is not a panacea. If an attacker gains system-administrator privileges, they may be able to get keys or disable encryption methods without a user's knowledge.

5.7 Intrusion Detection and Computer Forensics

Logging records the events on a computer system or network. This can generate enormous amounts of data, so intrusion-detection systems can be set up to check and record just the events that might indicate an attack, alerting system administrators when matters become serious. IDSs can be located on individual or on networks. They are important defensive tools against a broad range of known attacks including Trojan horses. Most look for or bit patterns of known attacks, but a few look for or statistically suspicious behaviour and thus can detect some new kinds of attacks. IDSs are useful but are not perfect since attackers try hard to disguise their attacks.

For new or complex attacks, computer forensics capabilities are needed, utilising methods for inspecting computer storage after an attack to determine how the attack was accomplished and what damage it did. Forensics includes a wide variety of techniques and requires an intelligent investigator to use considerable judgment. Thus, it requires time and can only be done after the attacker is gone.

5.8 Honeypots

Honeypots and honeynets (networks of honeypots) provide richer log information about cyber-attacks. These are systems with no legitimate purpose other than to receive attackers, so everyone using them other than their system administrator is inherently suspicious. Honeypots need not explicitly invite attackers once they are on the Internet, attackers can find them with automated tools. However, they can be dangerous if attackers use them as springboards to attack other sites. For this reason, reverse firewalls of various kinds must keep the attack from spreading. But an attacker may infer the existence of the honeypot from the restrictions of the reverse firewall, so a honeypot cannot remain effective forever.

5.9 Intrusion Prevention Systems

Most of the methods discussed so far just react to attacks. The alternative is an active network defence, which in its simpler forms is called an intrusion-prevention system. This includes simple things like turning off the Internet connection or logging out a user when they become sufficiently suspicious as judged by an intrusion-detection system. It can also include forms of limiting damage such as denying the user certain resources, downgrading their priority, or delaying them.

5.10 Back Tracing

Back tracing is a form of active network defence that tries to find where an external attack is coming from so as to stop it more easily. Back tracing is virtually impossible with serious attackers, who take care to come in via a long sequence of sites through many countries and jurisdictions; it is hard to get the cooperation of all those jurisdictions.

5.11 Counterattacking

A more irresponsible form of active network defence is trying to counterattack whatever machine is attacking you. However, this won't work against insiders. Since most serious attacks use intermediate machines to attack yours, such a response will often only hurt a site or computer that is an innocent bystander. Even if it works and you do hurt the attacker, attacks could easily escalate with resultant collateral damage.

5.12 Deception

Deliberate deception has also been proposed for active network defence. Systems could lie, cheat, and mislead attackers to prevent them from achieving their goals. Deception is particularly useful for time-critical military-style attacks such as those by cyber-terrorists or information-warfare experts, when just delaying an attack a while could buy time to find a more permanent defence. Deception has been used in honeypots to keep the attacker interested. Fake files can be put on a honeypot to make it look more like a normal machine, and fake sites can be programmed to respond like real network nodes. Deception is equally useful against insider and outsider attacks.

In regard to external countermeasures, as they involve an act, in that there are in response to an act committed unlawfully against the victim state, there are strict conditions that need to be met. The countermeasure may not be conducted until the injured state has notified the state responsible that it intends to take countermeasures and gives the responsible state an opportunity to desist in its unlawful conduct. However, in the context of a cyber response, the notification requirement is subject to a condition of feasibility, as the advanced notification of an impending cyber countermeasure could allow the responsible state to foil such a response.

The countermeasures should also be proportionate to the injury to which they respond. They have to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the right question". There may be provisions in treaties that detail the taking of specific responses in the even of breaches, if so, the injured state much resort to them before taking any countermeasures.

Operationally, countermeasures that are utilised also do not need necessarily need to be "in-kind" nor directed at the entity that authored the internationally wrongful act. A state victim of an attack may response with cyber measures that the sovereignty of the responsible state, for example. This is reflected in maritime law, where a state that has been targeted by another state's unlawful cyber operations would be entitled to close its territorial sea to vessels of the responsible state, that are transiting in innocent passage. Another cyber response to an attack could be to direct the response at private corporations within the responsible state, so long as the response and operations are proportionate to the originating attack and comply with the requirements of countermeasures.

6 Conclusion

As critical national infrastructure utilises emerging technologies in order to maximise efficiency and effectivity, it also opens up these critical networks and systems to non-conventional cyber-attacks. The threat landscape is as complex as the system itself, with vulnerabilities open for exploitation by both independent operators, rogue state operatives, state backed threat actors and state mechanisms themselves. Such is the benefit of utilising cyberoperations mechanisms in terms of speed, impact and minimising human impact by means of the deliverer of the attack vector, that cyber capabilities are now a ratified capability in many nations globally. It is imperative that a greater understanding of both the implications of an sustained attack, and the results of perpetrating a cyber attack filtered into the legislative and governance mechanisms of nation states, and that agreed conventions and law defining peace and wartime mechanisms is adhered to, and understood in the context of a cyber war.

Bibliography

1. 3GPP (2017) SA3-security. The Third Generation Partnership Project (3GPP)
2. Agiwal M, Roy A, Saxena N Next generation 5G wireless networks: a comprehensive survey. IEEE Commun Surv Tutor 18(3):1617–1655. thirdquarter 2016
3. Akghar B, Yates SJ (2011) Strategic intelligence management for combating crime and terrorism. In: Akhgar B., Yates S. (eds) Intelligence Management. Advanced Information and Knowledge Processing. Springer, London
4. Alliance N (2015) NGMN 5G white paper. Next generation mobile networks, White paper
5. Cook A, Smith R, Maglaras L, Janicke H (2016) Measuring the risk of cyber attack in industrial control systems. BCS eWiC
6. Cook A, Nicholson A, Janicke H, Maglaras L, Smith R Attribution of cyber attacks on industrial control systems. EAI Endors Trans Ind Netw Intell Syst 3(7):151158
7. Cyber attack led to bristol airport blank screens. https://www.bbc.com/news/uk-england-bristol-45539841
8. Energy sector on alert for cyber attacks on UK power network. https://www.ft.com/content/d2b2aaec-4252-11e8-93cf-67ac3a6482fd. Accessed on 5 Feb 2018
9. Ericsson GN (2010) Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans Power Deliv 25(3):1501–1507
10. Evans M, He Y, Maglaras L, Janicke H (2018) Heart-is: a novel technique for evaluating human error-related information security incidents. Comput Secur
11. Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2018) A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustain Cities Soc 38:806–835
12. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H (2018) Security for 4g and 5g cellular networks: a survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl 101:55–82
13. Freudiger J, Manshaei MH, Hubaux J-P, Parkes DC (2009) On noncooperative location privacy: a game-theoretic analysis. In: Proceedings of the 16th ACM conference on computer and communications security, ser. CCS '09. ACM, New York, pp 324–337
14. Fujita H, Gaeta A, Loia V, Orciuoli F (2018) Resilience analysis of critical infrastructures: a cognitive approach based on granular computing. IEEE Trans Cybern:1–14
15. Geraci G, Dhillon HS, Andrews JG, Yuan J, Collings IB (2014) Physical layer security in downlink multi-antenna cellular networks. IEEE Trans Commun 62(6):2006–2021
16. Gope P, Hwang T (2016) Bsn-care: a secure iot-based modern healthcare system using body sensor network. IEEE Sensors J 16(5):1368–1376
17. Huawei (2016) 5G security: forward thinking. Huawei, Technical .report
18. Knapp ED, Langill JT (2014) Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Syngress, Waltham
19. Kulkarni P, Khanai R, Bindagi G (2016) Security frameworks for mobile cloud computing: a survey. In: 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT), pp 2507–2511
20. Maglaras LA, Jiang J (2014) Intrusion detection in SCADA systems using machine learning techniques. In: Science and information conference (SAI), IEEE, pp 626–631
21. Maglaras LA, Kim K-H, Janicke H, Ferrag MA, Rallis S, Fragkou P, Maglaras A, Cruz TJ (2018) Cyber security of critical infrastructures. ICT Express 4(1):42–45
22. Nicholson A, Watson T, Norris P, Duffy A, Isbell R (2012) A taxonomy of technical attribution techniques for cyber attacks. In: European conference on information warfare and security, p 188
23. ONF (2013) SDN security considerations in the data center. Open Networking Foundation
24. Panayiotou CG, Ellinas G, Kyriakides E, Polycarpou MM (2016) Critical information infrastructures Security. Springer, Berlin/Heidelberg

25. Petit J, Shladover SE (2015) Potential cyberattacks on automated vehicles. IEEE Trans Intell Transp Syst 16(2):546–556
26. Pipyros K, Thraskias C, Mitrou L, Gritzalis D, Apostolopoulos T (2018) A new strategy for improving cyber-attacks evaluation in the context of Tallinn manual. Comput Secur 74:371–383
27. Polla ML, Martinelli F, Sgandurra D A survey on security for mobile devices. IEEE Commun Surv Tutor 15(1):446–471. First 2013
28. Ralston PAS, Graham JH, Hieb JL (2007) Cyber security risk assessment for SCADA and DCS networks. ISA Trans 46(4):583–594
29. Robinson M, Jones K, Janicke H (2015) Cyber warfare: issues and challenges. Comput Secur 49:70–94
30. Robinson M, Jones K, Janicke H, Maglaras L (2018) An introduction to cyber peacekeeping. J Netw Comput Appl 114:70–87
31. Robinson M, Jones K, Janicke H, Maglaras L (2018) Developing cyber peacekeeping: observation, monitoring and reporting. Gover Inform Q 36(2):276–293
32. Rye dam attack. https://www.newsweek.com/cyber-attack-rye-dam-iran-441940
33. Saalbach K (2017) Attribution von cyber-attacken – methoden und praxis
34. Schmitt MN (2013) Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, Cambridge
35. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J (2018) A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commu Surv Tutor 20(4):3453–3495
36. Ten C-W, Manimaran G, Liu CC (2010) Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans Syst Man Cybern Part A Syst Hum 40(4):853–865
37. Ukraine cyber attack energy. https://www.wired.com/story/crash-override-malware/
38. Vikas SS, Pawan K, Gurudatt AK, Shyam G (2014) Mobile cloud computing: security threats. In: 2014 international conference on electronics and communication systems (ICECS), pp 1–4
39. Wolf creek nuclear plant hit cyberattack. https://www.theenergytimes.com/cybersecurity/wolf-creek-nuclear-plant-hit-cyberattack
40. Zonouz SA, Rogers KM, Berthier R, Bobba R, Sanders WH, Overbye TJ (2012) Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans Smart Grid 3(4):1790–1799