ICIC Express Letters
Part B: Applications
Volume **11**, Number **11**, November **2020**

ICIC International ©2020 ISSN 2185-2766
pp. 1019–1028

CYBER SECURITY: BETWEEN CHALLENGES AND PROSPECTS

Mwaffaq Abu-Alhaija

Department of Networks and Information Security
Al-Ahliyya Amman University (AAU)
P.O. Box 119, Amman 19328, Jordan
m.abualhija@ammanu.edu.jo

Received March 2020; accepted June 2020

Abstract. *This research studies the severe challenges facing cyber security which are thrown due to the growth of Internet technology. In this paper, cyber security is studied in a wide range of domains, from infrastructure, to networks, to databases, to applications, to identity and access management, as well as cloud systems and the Internet of Things. Bridging the gaps between these domains has become essential to address cyber security risks. Different focus by each organization and provider in the Cyberspace on relevant security domains has resulted in a disjointed state of security for the Cyberspace. Furthermore, a Disaster Recovery plan needs to be firmly in place as part of an overall Business Continuity Strategy to mitigate loss and disruption. Therefore, the search for methods to ensure cyber security, as well as the development of appropriate technologies, has become an important aspect of the IT sector. In conclusion, cyber security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.*

Keywords: Cyber security, Cyberspace, Cybercrime, Information system, Cyber-attacks, Disaster Recovery, Cyber security awareness, Infrastructure security, Network security, Database security, Application security, Identity and access management, Cloud security

1. **Introduction.** Understanding all the basic elements of cyber security is the first step for organizations in order to face the threats to their information systems and data. Cyber security focuses on protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible. It represents the ability to defend against and recover from accidents, as well as from attacks by adversaries. The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical Information and Communications Technology (ICT) devices and connected networks [1]. Cyber security consists of technologies, processes and controls designed to protect systems, networks, programs, devices and data from cyber-attacks. However, there are security issues that are not enclosed in the current security measures, from information security, to Internet security, to network security and ICT security. Due to the gaps between these domains, as well as the lack of communication between organizations and providers in the Cyberspace, it has become essential to bridge the gaps between the different security domains in the Cyberspace and address common cyber security risks.

A fragmented state of security for the Cyberspace has resulted due to different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider. Nowadays, news

DOI: 10.24507/icicelb.11.11.1019

about cybercriminals comes daily as they seize control of other people's computers, gadgets, software, or launch relevant programs against specific sites, information resources, or certain mobile app content. Therefore, in many countries, increasing attention is being paid to cyber security. Information security and digitalization nowadays penetrate all scopes of activity whether in a state, society, business, science, education, and even the individuals. Therefore, the search for methods to ensure cyber security, as well as the development of appropriate technologies, has become an important aspect of the IT sector.

The purpose of the article is to study and consider the general problems of cyber security. The article discusses the interpretation of the concepts of Cyberspace and cyber security, related to both organizational and technical aspects. The article also addresses and investigates the main problems of cyber security and considers possible prospects and solutions.

2. **Problems Facing Cyber Security.** The recent findings, as documented in government reports [3,4], indicate the growing threat of physical and cyber-based attacks in numbers and sophistication on electric grids and other critical infrastructure systems. The growth of Internet technology has thrown severe challenges in form of requirement of a suitable cyber defense system to safeguard the valuable information stored on system. Over the years, coupled with technological development and need, Internet technology has grown, offering numerous functionalities and facilities. Protecting the Internet and Internet users has become integral to the development of new services as well as governmental policy. Towards this goal it is proposed to study and understand the various malicious objects. The three modes of malicious attacks on any infrastructure are as follows: 1) attack upon the system; 2) attack by the system; and 3) attack through the system [2].

The fight against cybercrime needs a comprehensive and a safer approach. Hence, an equally comprehensive understanding of the numerous areas of cyber security is essential. Without a full realization to all areas covered by cyber security, any cyber defense strategy will remain susceptible to vulnerabilities. As the scope of cyber security is broad, any good cyber security strategy should take them all into account. The core areas are described in Figure 1.

2.1. **Cyber security as a global challenge.** Cyber security can no longer be perceived as a pure computer security issue, but rather as a national policy matter due to the illicit use of Cyberspace could hamper economic, public health, safety and national security

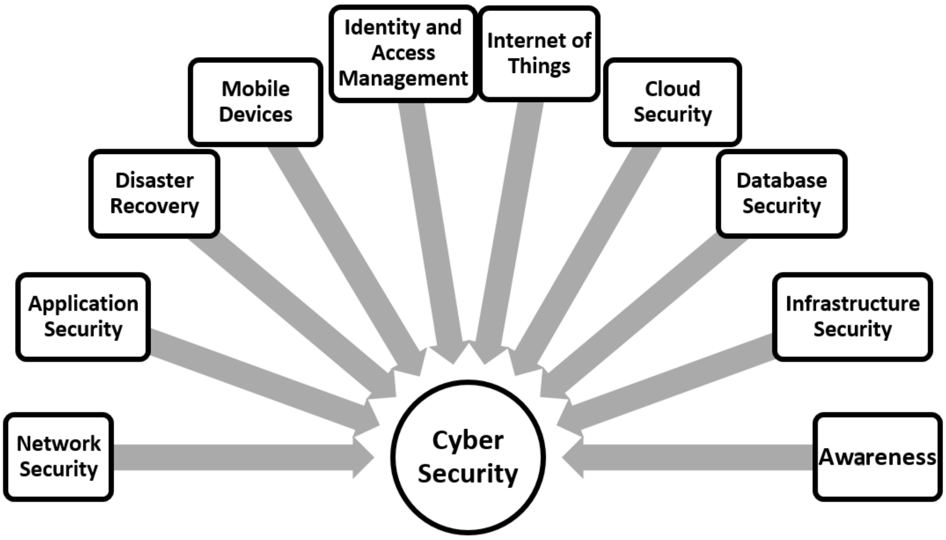


FIGURE 1. The domain areas of cyber security

activities. National leaders have accountability for devising a cyber security strategy and fostering local, national and global cross-sector cooperation. Since technical measures alone cannot prevent any crime, it is critical to allow law enforcement agencies to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities to prevent the loss of important information. Cyber space poses unique difficulties due to the global reach of ubiquitous networks that usually span over jurisdictions with weak laws and/or no enforcement, as well as the fast connection speeds giving victims little time to defend against attacks.

2.2. **Critical infrastructure security.** Critical infrastructure includes the cyber-physical systems that society relies on, including the electricity grid, water purification, traffic lights and hospitals. Whilst what comprises critical infrastructure varies across nations, typical infrastructure sectors include health, water, transport, communications, government, energy, food, finance and emergency services sectors. Although the complex infrastructure provides great capabilities for operation, control, business, and analysis, it exposes it to a large set of risks from either natural or human sources, becoming at increasing risk of a malicious cyber-attack. Effective protection against these attacks requires flexible solutions that can adapt to their unique industrial contexts and challenges while being strong enough to keep out even the most persistent or advanced adversary.

All the critical infrastructure sectors rely upon physical infrastructure such as buildings, roads, plants and pipes. Increasingly, the critical sectors also rely on Cyberspace and the Information and Communication Technologies (ICTs) that enable it. The Critical Information Infrastructure (CII) operates and controls the critical sectors and their physical assets. Consequently, ensuring the reliable functioning of Cyberspace is a strategic national objective because the lack of trust and confidence in the use of ICTs could hinder daily life, commerce and national security.

Electronic security is as important as physical security due to the potential impact that can be made through operations of critical cyber assets. The evolution of Supervisory Control and Data Acquisition (SCADA) systems has also raised concerns about cyber-related vulnerabilities [6]. SCADA systems are one of the most critical industrial systems because of their functionality in supervising and controlling large and worldwide industrial networks, such as electricity and gas distribution networks [7]. In addition, interdependences among computers, communication, and power infrastructures have increased the risks due to complexity of the integrated infrastructures [8]. While technological advances can help to reduce the deficiencies of current power and communication systems [9], technological complexity can also lead to security breaches that are prone to electronic intrusions. A successful intrusion into the control networks can lead to undesirable switching operations executed by attackers, resulting in widespread power outages. Other potential scenarios are intrusion into one or more substations and alteration of the protective relay settings, which could result in undesirable tripping of circuit breakers.

Most cyber defense systems create overheads like slow down the existing system performance, increase the packet length or take more time for comparison. So it is needed to provide such a cyber-defense system, which does not create much more extra overheads. Both defensive systems (after attack recovery, and before attack) should be predictable enough on the basis of mathematical modeling with high accuracy. Hence, to manage all these risks, a powerful risk management framework is needed to predict the most significant risks and handle them correctly. The recent works in [7] and [8] are examples of such proposed models.

2.3. **Network security.** Network security guards against unauthorized intrusion as well as malicious insiders. Ensuring network security often requires trade-offs. For example, access controls such as extra logins might be necessary, but slow down productivity. Network security is used to protect the networking components, connection of networks and content related to network, and typically relies on layers of security and it consists of more than one component that include in to the network for monitoring network and security software and hardware, and its appliances. All components work together to increase the overall security and performance of the computer network.

Network segmentation allows partitioning into multiple segments with limited access to each other so that risk is mitigated from attacks like “land and expand” ransomware variants. A properly configured firewall is a critical part of perimeter security. Changes to the firewall need to be evaluated for security vulnerabilities. Refrain from using default passwords with network equipment, and change passwords immediately after support personnel are terminated. All end-user devices of a computer network should be securely configured and encrypted, supported operating systems and have updates and patches applied as soon as they are available.

2.4. **Mobile devices.** There is no use of diligence in protecting access to sensitive data if employees are utilizing unsecure mobile devices, such as laptops and smartphones, which easily access the network. Moreover, most companies supply their visiting customers or vendors with access to Wi-Fi. Consequently, most cybercrime is now mobile; over 60% of online fraud is accomplished through mobile platforms, and 80% of mobile fraud is carried out through mobile apps instead of mobile web browsers [5].

With poor user awareness and/or behavior, users could unknowingly buy infected hardware, suffer of device hijacking, or even end up losing their devices. The most common risks that are associated with the use of mobile devices have varying impact on security of the cyber space in which they are used. What amplifies the issue is the lack of preparedness: 67% of organizations confessed they are less confident about the security of their mobile assets than other devices in their network [11].

2.5. **Identity and access management.** Humans have responsibility to ensure the Confidentiality, Integrity, and Availability (CIA) of their organizational and personal computer systems [10]. Controlling access to the campus, building and areas that contain sensitive data are a high security concern. Ultimately the aim of any cybersecurity solution is to control who and what has access to your applications and data, and this sits at the core of Identity and Access Management. Funding for Identity and Access Management (IAM) projects is not always a priority because they do not directly increase either profitability or functionality. However, identity and access management addresses the critical requirement of ensuring appropriate access to resources across increasingly heterogeneous technology environments. Identity management [9] should include identification and authentication of people and devices, physical and logical assets control, access control attacks and mitigation measures, and Identity as a Service (IaaS).

It is not enough to simply restrict access to full-time company employees. It is also critical to ensure that only authorized individuals have access to the network and data. It is critical to ensure that only authorized individuals have physical access to these areas. Identity Access Management (IAM), Rules-based Access Control (RAC), Roles-Based Access Control (RBAC) [11], and identity creation methods help increase security with access control depending of what type of user ID an authorized individual is issued. IAM ensures only authenticated individuals can access a network and controls and limits the information these individuals can access. Essentially, IAM measures enable the ‘right resources’ to be accessed by the ‘right individuals’ at the ‘right times’ and for the ‘right reasons’. Access controls such as photo ID badges, least-privilege permissions for badge access, security cameras, a policy that requires guest check-in, are all important examples of physical access controls any business should consider implementing.

Controls such as least-privilege permissions for end-user access to the network, periodic reviews of access permissions, and the immediate removal of access due to role change or termination are especially important to a comprehensive security plan. Identity management as a service (e.g., Cloud identity) brings forward issues such as the system being out of the user's control with no way to know what has happened to the information in the system, auditing access, ensuring compliance and flexibility to quickly revoke permissions.

2.6. **Application security.** The Software and Application Security knowledge area focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects [11]. The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software and applications depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. Some applications are more susceptible to threats than others. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

The Software and Application Security knowledge area addresses these security issues. The knowledge units within this knowledge area are composed of fundamental principles and practices. It has become crucial to address essential principles to avoid software security design flaws [12]. Fundamental design principles include least privilege, open design, and abstraction, while security requirements and their role in design should be clearly identified. Implementation issues, as well as configuring and patching should undergo thorough testing, both statically and dynamically. Moreover, the ethical perspective should be precisely considered, especially in development, testing and vulnerability disclosure.

2.7. **Cloud security.** The enterprise's move into the cloud creates new security challenges [15]. On the one hand, this can make security easier for companies outsourcing their data to lie on a cloud service where the cost of security is carried by the vendor, but on the other hand, it centralizes cloud services as highly viable targets for attack. The main issue with cloud computing is that it is the 'third-party' element that is been responsible for a lot of the reluctance to adopt cloud services in the past. Many believe that their data would be less secure because their server is not in the same building as they are, based on the loss of physical access to the server hosting their data. In fact, data centers employ individuals who have much more specialized knowledge in terms of security and safety measures for server and data protection [16]. Large multi-billion organizations can afford to dedicate specialist resources to the single task of server security and even the most dedicated in-house team will not be able to match the knowledge and skill level of large cloud computing providers.

Security of cloud data is not just about encryption, but also the authority of access when data is physically located in an overseas jurisdiction [15]. Cloud security software is a critical component of a comprehensive cybersecurity strategy. Regardless of whether a server is on or off premises, cloud cyber security requires both on-premises software and cloud-based software that sit between service users and cloud applications. This software monitors all user activities, warns administrators about potentially hazardous actions, enforces security policy compliance, and automatically prevents malware. Cloud providers are continuously creating new security tools to help enterprise users better secure their data. Furthermore, cloud service providers carry out much more thorough background checks on employees who have physical access to servers. The Internet may have no borders, but data itself still lies within traditional real-world boundaries and in turn may be bound by the laws of a foreign nation. Regardless of the trustworthiness of the current laws of a foreign nation there is no guarantee they will not change, and data that was previously protected could be subpoenaed, accessed by government departments, or shared with third parties without consent. While cloud service providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) continue to expand security services to protect their evolving cloud platforms, it is ultimately the customers' responsibility to secure their data within these cloud environments [16]. Various recent security reports [13,15,16] emphasize that cloud security teams must reassess their security posture and strategies, and address the shortcomings of legacy security tools to protect their evolving IT environments. Cloud security could possibly remain a major concern and the bottom line remains: Moving to the cloud is not a remedy for performing outstanding industry when it comes to cyber security.

2.8. **Database security.** Database security covers and enforces security on all aspects and components of a database. Database security is generally planned, implemented and maintained by a database administrator or other information security professional. Data-centric security measures focus on the security of the data itself as opposed to data access measures which focus on the security of networks, servers, or applications. Database cybersecurity measures include restricting unauthorized access to data on a database, but also the physical security of the server and backup equipment in case of theft or damage. Some key components of this area of cybersecurity include implementing strong and multifactor authentication to better control who has access to your data, as well as reviewing and mapping out known vulnerabilities. Load and stress testing should also be carried out to ensure that a database will not crash during Distributed Denial of Service (DDoS) attacks or user overload.

Organizations should always aim for 'least privileges' which means end-users and administrators should always only have the minimum number of privileges required in order to do their job, and only at the times that they need access. It is often the case that users accumulate privileges as they move through organizations, (also known as privilege creep). Investment in strong access management products can help prevent far greater costs later down the line from security incidents and data breaches that are caused by privilege creep.

2.9. **Internet of Things security.** The security challenges and security threats to IoT must be recognized for protective action to be taken. The overall goal should be to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT. With many security challenges identified, such as confidentiality, privacy and entity trust, it has been clear that security and privacy challenges need to be addressed. Furthermore, current research should address extra focus upon the cyber threats comprising actors, motivation, and capability fuelled by the unique characteristics of Cyberspace.

It is important for upcoming standards to address the shortcomings of current IoT security mechanisms [13]. As future work, the aim is to gain deeper understanding of the threats facing IoT infrastructure as well as identify the likelihood and consequences of threats against IoT. Definitions of suitable security mechanisms for access control, authentication, identity management, and a flexible trust management framework should be considered early in product development. The major issues in IoT security should be thoroughly addressed providing better understanding of the threats and their attributes originating from various intruders like organizations and intelligence agencies.

2.10. **Cyber security awareness.** In cyber defense it is difficult to trace the attacker due to lower education and awareness. The weakest link in a company's cybersecurity chain is typically its people, and mainly due to a lack of awareness, employees frequently open the gates to attackers. Security awareness for emerging technologies is critical to prevent cyber-attacks. Only few countries have some adequate policies, and education and awareness system. Therefore, to restrict such type of malicious activities, our society needs to devise a proper set of policies. A proper cyber security defense strategy should assign responsibility to coordinate cyber security awareness campaigns and activities at the national level to a competent authority to ensure resources are streamlined and accountability established. Cyber security awareness promotes foundational understandings on cyber threats and risk, cyber hygiene, and appropriate response options. It informs citizens on best practices and proactive measures when confronted with cyber risks. The authority should collaborate with relevant stakeholders to develop and implement cyber security awareness programs focusing on disseminating information about cyber security risks and threats, as well as about best practices for countering them. Nations should promote cyber awareness of cyber-related threats among the public, companies and government employees.

A cyber security awareness-raising program could include awareness-raising campaigns aimed at the general public, children, digitally challenged, consumer-focused education programs, and awareness-raising initiatives among others, targeted at executives across public and private sectors. End-user education is about educating your employees but also checking and testing that they follow the advice that they are given. End-user education will help to prevent the risk of human error; however, it is impossible to eliminate the risks completely. Every individual must also be trained on this cyber security and save themselves from these increasing cyber-crimes.

2.11. **Disaster Recovery and incident response.** Even with protective and proactive cyber security solutions, networks and data can still be breached. Maybe an absent minded or disgruntled employee has been using poor password hygiene or curiosity got the better of them and they clicked on a corrupt link in a phishing email. When it comes to cybersecurity, government recommendations lean towards proactive rather than reactive measures, but what happens if disaster strikes? By not focusing enough resources on Disaster Recovery or Business Continuity planning, an organization leaves itself vulnerable, meaning its existence could be threatened. Since the forces that govern the business marketplace have shifted considerably in the past decade, the importance of Disaster Recovery cannot be understated or underestimated accordingly. Disaster Recovery is an integral part of overall risk management for organizations small and large alike. It is no longer a case of "if it will happen", more like "when it happens". Unfortunately, that is the mindset that business leaders need to accept to fully grasp the realities of the situation. In the event of a disaster, the continued operations of an organization depend on the ability to replicate IT systems and data in quick time to mitigate loss and disruption.

The importance of Business Continuity Planning is something that almost every organization has been forced to deal with due to not just recent events, but doing business in the new age altogether. The ability of an enterprise to recover from disaster is directly related to the degree of Business Continuity Planning (BCP) that has taken place before the disaster. Crucial keyword is "before". With an organization's reputation on the line, it is necessary to allocate sufficient resources to Business Continuity in the case of a disaster. Organizations need to take the necessary steps to mitigate risk and loss due to Cyber Security threats. Furthermore, a Disaster Recovery plan needs to be firmly in place as part of an overall Business Continuity Strategy. Even when plans are put in place, testing of Contingency Plans also needs to follow suit. All strategic planning must stay moving with rigorous testing and improving the plan as you go along patching up all points of vulnerability.

3. **Disscusion.** Cyber security is a never-ending battle. While most cyber security problems result from the inherent nature of Information Technology (IT), the complexity of information technology systems, and human fallibility, a permanently decisive solution to the problem will not be found in the foreseeable future. In addition, as new defenses emerge to stop older threats, intruders adapt by developing new tools and techniques to compromise security. As innovation produces new information technology applications,

new opportunities for criminals, terrorists, and other hostile parties also emerge, along with new vulnerabilities that malicious actors can exploit. Thus, adversaries, especially at the high-end part of the threat spectrum, constantly adapt and evolve their intrusion techniques, and the defender must adapt and evolve as well.

Support for research in cyber security has expanded significantly, public awareness is greater than it was only a few years ago. Ultimately, the relevant policy question is not how the cyber security problem can be solved, but rather how it can be made manageable.

Improvements to cyber security call for two distinct kinds of activity: (a) efforts to more effectively and more widely improve current knowledge of cyber security, and (b) efforts to develop new knowledge and measures regarding cyber security. Improvement to existing technologies and techniques – and indeed the development of entirely new approaches to cyber security – is the focus of traditional cyber security research. A properly responsive research program is broad and robust, and it addresses both current and possible future threats. Knowledge about new cyber security technologies, techniques, tactics, organizational arrangements, and so on will help to strengthen defenses against an ever-evolving threat.

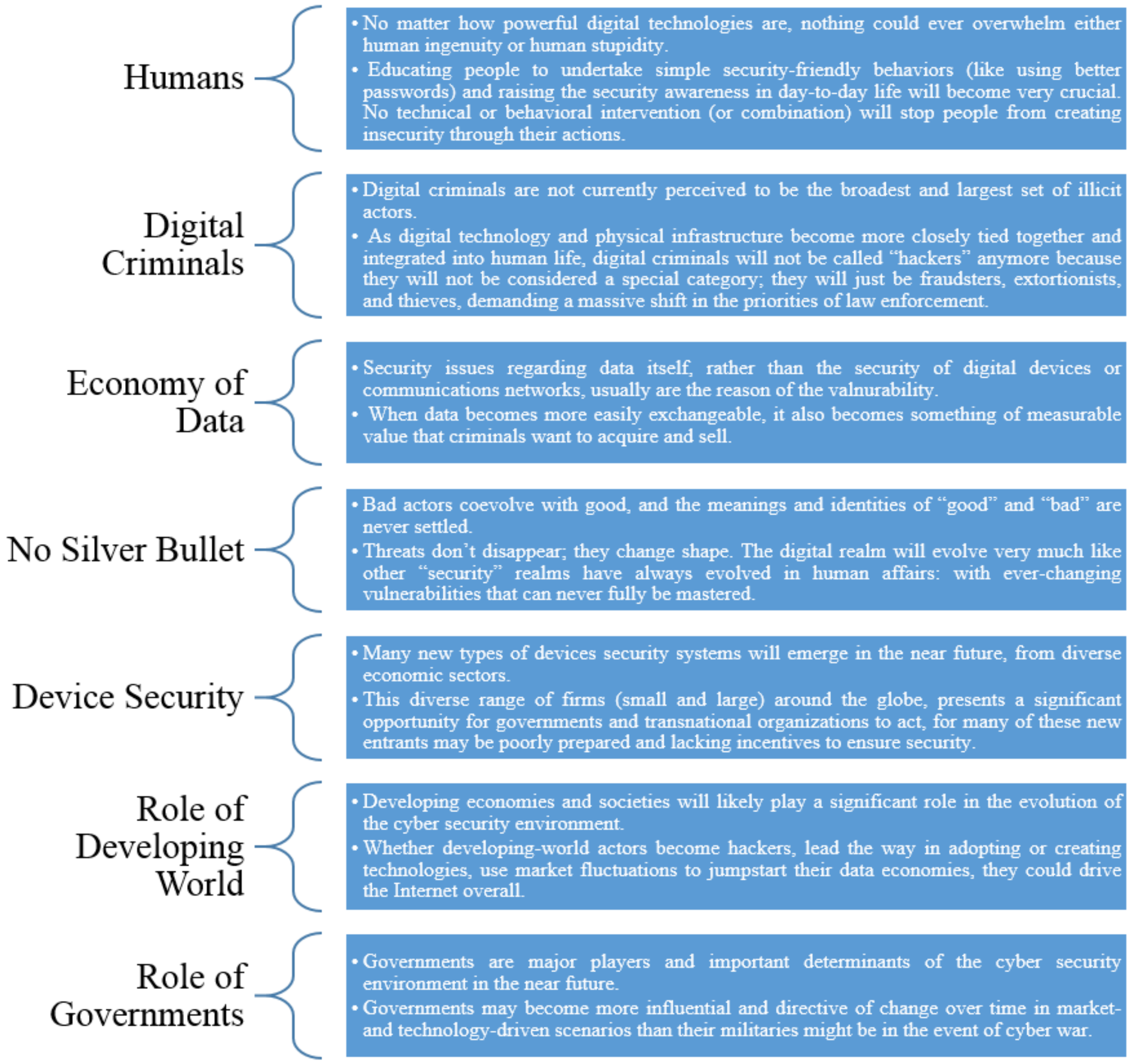
Although cyber security is important to nations worldwide, most nations have other more imperative necessities as well, some of which may conflict with the requirements of cyber security. Tradeoffs are inevitable and will have to be accepted through the nation's political and policy-making processes. Questions of prioritization play heavily in the conduct of foreign relations as well. In an environment of many competing priorities, reactive policy making is often the outcome. Support for efforts to prevent a disaster that has not yet occurred is typically less than support for efforts to respond to a disaster that has already occurred. In practice, although technical measures are an important element, cyber security is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details. That is a very different and much broader agenda for cyber security than what is found today.

The final insights perceived by this research are a summary that prompt expansive thinking and discussion in the sense that they generate more bold research ideas and creative policy propositions than fixed emphatic proclamations about what must or must not be done. These insights, presented as a way to provoke further thinking about the meaning of cyber security and its implications in an unseen future in Figure 2, could have different levels of significance for different readers.

4. Conclusion.

While many attacks are easily prevented by performing basic security tasks, referred to as "cyber hygiene", an attacker will always exploit the weakest link. An enterprise has a duty to include basic cyber security precautions. The least required measures include maintaining strong authentication practices, and not storing sensitive data where it is openly accessible. A good cyber security strategy needs to go beyond the basics. For most companies, the number of ways an attacker can gain entry to a system is expanding. Currently, the information and the physical worlds are merging, the Integrity, Confidentiality and/or Availability (ICA) of cyber-physical systems can now be threatened by criminals and nation-state spies. Devices such as cars, power plants, medical devices, even a smart fridge are becoming more and more vulnerable. Similarly, the trends toward cloud computing, Bring Your Own Device (BYOD) policies in a workplace, and the expansion of IoT create new challenges.

In conclusion, cyber security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. The cyber security world of the future will still be talking about malware, firewalls, network security, and social engineering. Furthermore, it will also be talking about personal memories, new



Humans

- No matter how powerful digital technologies are, nothing could ever overwhelm either human ingenuity or human stupidity.
- Educating people to undertake simple security-friendly behaviors (like using better passwords) and raising the security awareness in day-to-day life will become very crucial. No technical or behavioral intervention (or combination) will stop people from creating insecurity through their actions.

Digital Criminals

- Digital criminals are not currently perceived to be the broadest and largest set of illicit actors.
- As digital technology and physical infrastructure become more closely tied together and integrated into human life, digital criminals will not be called "hackers" anymore because they will not be considered a special category; they will just be fraudsters, extortionists, and thieves, demanding a massive shift in the priorities of law enforcement.

Economy of Data

- Security issues regarding data itself, rather than the security of digital devices or communications networks, usually are the reason of the valnurability.
- When data becomes more easily exchangeable, it also becomes something of measurable value that criminals want to acquire and sell.

No Silver Bullet

- Bad actors coevolve with good, and the meanings and identities of "good" and "bad" are never settled.
- Threats don't disappear; they change shape. The digital realm will evolve very much like other "security" realms have always evolved in human affairs: with ever-changing vulnerabilities that can never fully be mastered.

Device Security

- Many new types of devices security systems will emerge in the near future, from diverse economic sectors.
- This diverse range of firms (small and large) around the globe, presents a significant opportunity for governments and transnational organizations to act, for many of these new entrants may be poorly prepared and lacking incentives to ensure security.

Role of Developing World

- Developing economies and societies will likely play a significant role in the evolution of the cyber security environment.
- Whether developing-world actors become hackers, lead the way in adopting or creating technologies, use market fluctuations to jumpstart their data economies, they could drive the Internet overall.

Role of Governments

- Governments are major players and important determinants of the cyber security environment in the near future.
- Governments may become more influential and directive of change over time in market- and technology-driven scenarios than their militaries might be in the event of cyber war.

FIGURE 2. Summary of cyber security insights

distinctions between what is public and private, the power of prediction, faith in public institutions, the provision of public good, psychological stability, the division of labor between humans and machines, coercive power (both visible and invisible), what it means for a human-machine system to have "intention", and more.

REFERENCES

[1] ISO/IEC 27032:2012(en), *Information Technology – Security Techniques – Guidelines for Cyber Security*, Accessed in 2018.

[2] C.-W. Ten, G. Manimaran and C.-C. Liu, Cybersecurity for critical infrastructures: Attack and defense modeling, *IEEE Trans. Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol.40, no.4, 2010.

[3] *Official Website of the Department of Homeland Security*, https://www.dhs.gov/topic/cybersecurity, Accessed on Jan. 10, 2020.

[4] *Australian Cyber Security Centre*, https://www.cyber.gov.au/, Accessed on Jan. 10, 2020.

[5] Symantec, *Internet Security Threat Report*, vol.24, 2019.

[6] H. H. Safa, D. M. Souran, M. Ghasempour and A. Khazaee, Cyber security of smart grid and SCADA systems, threats and risks, *CIRED 2016*, Helsinki, DOI: 10.1049/cp.2016.0692, 2016.

[7] A. M. Elhady, H. M. El-bakry and A. A. Elfetouh, Comprehensive risk identification model for SCADA systems, *Security and Communication Networks*, https://doi.org/10.1155/2019/3914283, 2019.

[8] M. Amin and B. F. Wollenberg, Toward a smart grid: Power delivery for the 21st century, *IEEE Power Energy Mag.*, vol.3, no.5, pp.34-41, 2005.

[9] F. F. Wu, K. Moslehi and A. Bose, Power system control centers: Past, present, and future, *Proc. of IEEE*, vol.93, no.11, pp.1890-1908, 2005.

[10] T.-T. Teoh, Y.-Y. Nguwi, Y. Elovici, W.-L. Ng and S.-Y. Thiang, Analyst intuition inspired neural network based cyber security anomaly detection, *International Journal of Innovative Computing, Information and Control*, vol.14, no.1, pp.379-386, 2018.

[11] CSEC2017 Joint Task Force, *Cybersecurity Curricula 2017*, Version 1.0 Report, CSEC2017, 2017.

[12] I. Arce et al., Avoiding the top 10 software security design flaws, *IEEE Computer Society Center for Secure Design (CSD)*, Tech. Rep., https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf, 2014.

[13] M. Abomhara and G. Køien, Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks, *Journal of Cyber Security*, vol.4, pp.65-88, DOI: 10.13052/jcsm2245-1439.414, 2015.

[14] EY Global Information Security, Is cybersecurity about more than protection?, *EY Global Information Security Survey*, 2018.

[15] R. Gedda, Data manipulation, *Cybersecurity – Threats, Challenges, Opportunities*, 2016.

[16] B. Kuerbis and F. Badiei, *Mapping the Cybersecurity Institutional Landscape*, Digital Policy, Regulation and Governance, https://doi.org/10.1108/DPRG-05-2017-0024, 2017.