Enhancing Cybersecurity for Industry 4.0 in Asia and the Pacific

The Economic and Social Commission for Asia and the Pacific (ESCAP) serves as the United Nations’ regional hub promoting cooperation among countries to achieve inclusive and sustainable development. The largest regional intergovernmental platform with 53 member States and 9 associate members, ESCAP has emerged as a strong regional think tank offering countries sound analytical products that shed insight into the evolving economic, social and environmental dynamics of the region. The Commission’s strategic focus is to deliver on the 2030 Agenda for Sustainable Development, which it does by reinforcing and deepening regional cooperation and integration to advance connectivity, financial cooperation and market integration. ESCAP’s research and analysis coupled with its policy advisory services, capacity building and technical assistance to governments aim to support countries’ sustainable and inclusive development ambitions.

The shaded areas of the map indicate ESCAP members and associate members.

Disclaimer:
The Asia-Pacific Information Superhighway (AP-IS) Working Papers provide policy-relevant analysis on regional trends and challenges in support of the development of the AP-IS and inclusive development. The findings should not be reported as representing the views of the United Nations. The views expressed herein are those of the authors. This working paper has been issued without formal editing, and the designations employed and material presented do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Correspondence concerning this working paper should be addressed to the email: escap-ids@un.org.

Contact:
Information and Communications Technology and Development Section
Information and Communications Technology and Disaster Risk Reduction Division
United Nations Economic and Social Commission for Asia and the Pacific
United Nations Building
RajadamnernNok Avenue
Bangkok 10200, Thailand
Email: escap-ids@un.org
Acknowledgements

This working paper was prepared by Bhavna Choudhury and Atsuko Okuda of the Information and Communications Technology and Development Section (IDS), under the general guidance of Tiziana Bonapace, Director, Information and Communications Technology and Disaster Risk Reduction Division of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). The working paper benefited from comments and suggestions shared by Dongjung Lee, Siope Vakataki ‘Ofa, Alexey Kravchenko, Min Sun Kim and Su Yeon Lim of ESCAP. The working paper also benefited from peer review by Alexandru Caciuloiu of the United Nations Office on Drugs and Crime, Bangkok Office. Special thanks to Tarnkamon Chantarawat and Sakollerd Limkriangkrai of IDS who provided research assistance.

October 2018

Cover Photo: Shutterstock
Table of Contents

Acknowledgements ................................................................................................................................. 3
List of Figures .............................................................................................................................................. 5
List of Tables .............................................................................................................................................. 5
Abbreviations and Acronyms ..................................................................................................................... 6
Executive Summary ................................................................................................................................... 7
1. Introduction ........................................................................................................................................... 9
2. Cyberattack Trends .............................................................................................................................. 12
   2.1 Financial Impact of Cyberattacks ................................................................................................... 18
   2.2 Political Impact of Cyberattacks ..................................................................................................... 21
   2.3 Related Trends in Cyberattacks ....................................................................................................... 22
   2.4 Detailed Analysis by Attack Type .................................................................................................... 23
3. Artificial Intelligence in Cyberattacks ................................................................................................. 30
4. Artificial Intelligence in Cybersecurity ............................................................................................... 33
   4.1 Machine Learning Applications in Cybersecurity .......................................................................... 33
   4.2 Limitations of Machine Learning .................................................................................................... 38
5. Internet of Things Security .................................................................................................................. 39
   5.1 Machine Learning in IoT Security .................................................................................................. 40
6. The Dark Web Marketplace ................................................................................................................ 41
7. The Way Forward ................................................................................................................................ 44
Annex A: Glossary ...................................................................................................................................... 47
Annex B: Broadband Connectivity is a Requirement for Cybersecurity .................................................. 51
List of Figures

Figure 1: Relationship between cyberactions ................................................................. 13
Figure 2: Sampling of security incidents by attack type, time and impact (2014-2016) ............... 15
Figure 3: Cyberattacks reported and verified by the media in Asia-Pacific countries (2013-2017) .... 16
Figure 4: Web-based cyberthreats logged in Asia-Pacific countries (third quarter of 2017) ............... 17
Figure 5: Average financial impact of a data breach ............................................................. 19
Figure 6: Financial impact by type of attack .......................................................................... 19
Figure 7: Number of records reported and verified as lost in Asia-Pacific countries (2013-2017) ....... 20
Figure 8: Identified IP addresses for ransomware distribution on the Internet (2015-2017) ............... 24
Figure 9: Phishing attacks reported and verified by the online community (2013-2017) ................. 27
Figure 10: Hack modes for website defacement (2014-2015) ...................................................... 28
Figure 11: Website defacement attacks in Asia-Pacific countries (2014-2015) ......................... 29
Figure 12: Number of instances by category in the dark web marketplace ................................. 42
Figure 13: Average cost requested for cyberattack services on the dark web marketplace .............. 43
Figure 14: Number of vendors offering cyberattack services in the dark web marketplace ............ 43

List of Tables

Table 1: Examples of cyberattack motivation categorization .................................................. 15
Table 2: Top five IP addresses with Mirai Botnet collected by honeypots ............................... 38
Table 3: Price range of hacked accounts on the dark web ....................................................... 41
Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AP-IS</td>
<td>Asia-Pacific Information Superhighway</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CIGI</td>
<td>Centre for International Governance Innovation</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial-of-Service</td>
</tr>
<tr>
<td>ESCAP</td>
<td>Economic and Social Commission for Asia and the Pacific</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IDS</td>
<td>Information and Communications Technology and Development Section (ESCAP)</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
</tbody>
</table>
Executive Summary

As of September 2017, there were 1.25 billion websites in cyberspace. Thanks to the concerted efforts by governments and other stakeholders in extending broadband connectivity, an increasing number of people across Asia and the Pacific have joined cyberspace. Although broadband expansion remains uneven, there is evidence that digital dividends brought by broadband connectivity, such as e-government, e-learning, e-health and e-agriculture, have started permeating into previously underserviced and unserved areas in the region. Today, Asia and the Pacific accounts for half of all Internet users in the world.

In the past few years, we have witnessed a number of emerging technologies, such as Artificial Intelligence (AI), Big Data analytics and Internet of Things (IoT), which are contributing to a “Fourth Industrial Revolution”. The first industrial revolution began with industries powered by steam and water; in the second, electricity made mass production possible; the third one was the digital revolution; and this fourth revolution builds on the third but is characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres.3

Recently, the upside gains and downside risks from the fusion of emerging technologies have started to surface. The gains are evident in the new business and employment opportunities driven by innovative products and services, while the risks include increasing sophistication in cyberattacks and exposure to cybersecurity vulnerabilities. For instance, in recent years, attacks on IoT have focused on critical infrastructure, including a German steel mill causing serious damage to its production network,4 and a Ukrainian power station resulting in 80,000 people losing power.5

Along with the advancement of technology, cyberattacks are becoming increasingly sophisticated. Malicious technological developments intended to disrupt and sabotage the digital and physical world have and will continue to be more widespread as more devices are connected to the Internet. There is, in fact, an upward trend in the number of cyberattacks on the digital and physical infrastructure. Over the years, the intensity, frequency and severity of cyberattacks have increased.

The term “cybersecurity” has different connotations depending on the concerned community. Enterprises, governments, institutions and individuals are faced with different issues and priorities when addressing cybersecurity. For policymakers and legislators, they need to enact laws, legislations, policies, regulations and guidelines to define responsibilities and ensure safety and security in cyberspace. But to do so effectively, they are required to understand the emerging technologies, including the risks and threats, as well as the opportunities. Policymakers and legislators also need to be able to strike a balance.

---

4 Kim Zetter, “A cyberattack has caused confirmed physical damage for the second time ever”, Wired, 8 January 2015. Available at https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
between safety and security, and privacy and freedom of speech, as well as ensure alignment with international norms and agreements.

Against this increasingly complex and challenging background, this working paper has been prepared to enhance awareness and understanding of cyberattacks and cybersecurity issues among policy- and decision-makers, regulators, academia, private sector companies, and civil society organizations in Asia and the Pacific. The paper uses data on cyberattacks collected by media, academia, governments, private sector companies, antivirus and cyberattack monitoring websites, and dark web data dumps. In the absence of comparable official data reported by governments and international institutions, the data presented in this paper has been collected from various online and offline sources and may not be comprehensive in geographical coverage and time series.

The working paper aims to support the implementation of the Asia-Pacific Information Superhighway (AP-IS), a regional broadband connectivity initiative that extends from Turkey to Kiribati. With the increasing availability of broadband connectivity and the advancement of technologies, the risks of cyberattack may rise across the region. It is hoped that this paper provides some insights and understanding of the nature and magnitude of cyberattacks, and contributes to policy discussions and dialogues for action towards enhancing cybersecurity. Furthermore, it intends to provide examples of AI-enabled solutions and measures developed to counter AI-facilitated cyberattacks.

Based on the findings from this study, the paper offers some preliminary recommendations for the way forward, as follows:

- Ensure the privacy of individuals. A global cyberprivacy index could be developed to track the extent to which countries are safeguarding their citizens’ privacy rights.

- Establish an incident reporting mechanism to monitor and assess the occurrences of cyberattacks and data breaches, including their nature, scope and impact, as well as details of the responses to incidents.

- Strengthen laws and legislations, and increase penalties for cyberattackers and hackers.

- Plan and implement digital safety and digital literacy initiatives, and develop digital safety and digital literacy indicators to better gauge the current state of cybersecurity awareness among individuals and organizations worldwide.

- Invest in cybersecurity research and initiatives. Regional cooperation and knowledge sharing would also be crucial for addressing the wide range of cyberthreats and risks.

- Promote cybersecurity best practices for individuals and organizations, such as clearing cache, regularly updating software and enabling two-factor authentication for account login.
1. Introduction

Modern society is becoming increasingly dependent on technology, in particular digital technology. The reliance and increasing importance of digital technology is evident in the expansion of cyberspace—1.25 billion websites are currently registered in cyberspace. As cyberspace becomes more integrated into government, society and the economy, and their dependence on technologies deepens, there is an increasing concern on the resilience and security of cyberspace in the context of increasing number of cyberattacks and call for strengthened cybersecurity.

Another interlinked trend is the development of Artificial Intelligence (AI). In the Asia-Pacific region, developed countries with better broadband infrastructure, resources and capacity are investing heavily in businesses built around AI, according to a report of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). In 2016, a significant increase in investment in research and development of “Fourth Industrial Revolution” products was observed, with large technology companies and startups spending between USD 20 billion and 30 billion. Although AI is still in the nascent stage, companies are rapidly developing and testing solutions to apply increasingly efficient algorithms to their operations and product and service development.

The volume of data generated is becoming a powerful asset. This data includes personal information, financial transactions, assets and infrastructure, government records, business operations, and accounts and strategies, to name a few. Developed countries already have a major portion of business operations and personal information on the cloud, whereas the developing world is catching up to build critical infrastructures.
physical and security infrastructure to support these new technologies. Countries with limited infrastructure, access, capacity and resources are being left behind, vulnerable to cyberattacks.

Along with the advancement of technology, cyberattacks are becoming increasingly sophisticated. Malicious technological developments intended to disrupt and sabotage the digital and physical world have and will continue to be more widespread as more devices are connected to the Internet. There is, in fact, an upward trend in the number of cyberattacks on the digital and physical infrastructure. Over the years, the intensity, frequency and severity of cyberattacks have increased.

With over 50 billion connected devices and global Internet traffic volume of 1.3 zettabytes (in 2016), there is a looming fear that critical physical infrastructure and facilities connected to the Internet, and assets stored digitally, can be quickly compromised in cyberattacks. Moreover, financial losses related to compensation for compromised data, lawsuits, and recovery from cyberattacks through rehiring and securing networks, are extremely high. One estimate by the World Bank concludes that losses from cyberattacks will reach up to USD 2 trillion worldwide in 2019.

The term “cybersecurity” has different connotations depending on the concerned community. Enterprises, governments, institutions and individuals are faced with different issues and priorities when addressing cybersecurity. For policymakers and legislators, they need to enact laws, legislations, policies, regulations and guidelines to define responsibilities and ensure safety and security in cyberspace. But to do so effectively, they are required to understand the emerging technologies, including the risks and threats, as well as the opportunities. Policymakers and legislators also need to be able to strike a balance between safety and security, and privacy and freedom of speech, as well as ensure alignment with international norms and agreements.

Against this increasingly complex and challenging background, this working paper has been prepared to enhance awareness and understanding of cyberattacks and cybersecurity issues among policy- and decision-makers, regulators, academia, private sector companies, and civil society organizations in Asia and the Pacific.

It presents key highlights of the latest trends and types of cyberattack, focusing on phishing, ransomware, botnets, website defacement and advanced persistent threats (APTs) that have caught headlines.

---

12 In 2016, Internet traffic reached 1.3 zettabytes. A zettabyte is 1,000,000,000,000,000,000,000 bytes of information. This is a 50 per cent increase from 2011 to 2014. If this trend continues, traffic will increase to 4.38 zettabytes by 2025. However, if there are advances in storage, more devices and more streaming, then traffic will likely exceed this. Julian Bunn, "How Big is a Petabyte, Exabyte, Zettabyte, or a Yottabyte?" High Scalability, 11 September 2012. Available at http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html; and Tom Butts, "Welcome to the Zettabyte Era", TV Technology, 23 June 2016. Available at https://www.tvtechnology.com/opinions/welcome-to-the-zettabyte-era.


worldwide in 2017. In addition, this paper examines the dark web marketplace, an area that may need to be studied in greater detail by the law enforcement community. Finally, based on the realities of the various risks and vulnerabilities, the paper reviews cybersecurity measures, policies and legislations of selected countries in the region, and proposes some key recommendations for consideration.

The working paper uses data on cyberattacks collected by media, academia, governments, private sector companies, antivirus and cyberattack monitoring websites, and dark web data dumps. The types of data collected include – broadband penetration, AI cybersecurity research patents, Internet of Things (IoT) security research patents, investments in information and communications technology (ICT) services, the Global Cybersecurity Index, and data centre security reports from various open source platforms. In the absence of comparable official data reported by governments and international institutions, the data presented in this working paper has been collected from various online and offline sources, and may not be comprehensive in geographical coverage and time series. The technical terminologies used in this paper are defined in a glossary in Annex A.
2. Cyberattack Trends

There is no apparent international consensus on the definition of the terms “cybercrime” and “cyberattack”. In recognition of the increasing importance of the topic, the United Nations Salvador Declaration in 2010\(^{15}\) invited the Commission on Crime Prevention and Criminal Justice to:

Consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

Subsequently, the United Nations General Assembly Resolution 65/230\(^{16}\) was adopted to further investigate and create guidelines on addressing cybercrime. However, there are no resolutions that have established the definitions and categories of cybercrime or cyberattack.

It is important to distinguish between “cybercrime” and “cyberattack”. Cybercrime is the broad umbrella under which actions that are performed using cyberplatforms are considered criminal under justice systems. This may include online child sexual exploitation, money laundering through cryptocurrencies, funding and promoting terrorist organizations, and using the dark web for selling drugs and related criminal services. For the purpose of this paper, “cybercrime” is defined as, “cyberactions performed by non-state actors that violate criminal law, and may or may not have a political or national security purpose”.\(^{17}\) This paper treats “cyberwarfare” as a separate category that involves state actors and is associated with activities related to armed conflict.

The paper limits the definition of cyberattacks to two main instances – “cyberactions performed by non-state actors to undermine the function of a computer network”,\(^ {18}\) and “threats breaching security controls around a physical or an information asset”.\(^ {19}\) Cyberattacks can be further categorized by state and origin as active or passive.\(^ {20}\) An “active” attack aims to alter system resources or affect their operation. Conversely, a "passive" attack seeks to use information from a system but does not affect system


\(^{18}\) Ibid.


\(^{20}\) Ibid.
resources. Instead, passive attacks aim to obtain data for an offline attack. The term “data breach” is used interchangeably with “cyberattack”. Figure 1 illustrates the relationship between cybercrime, cyberattack and cyberwarfare.

Figure 1: Relationship between cyberactions

Cyberattacks are on an upward trend. The Breach Level Index developed by a private company, Gemalto, shows that the number of data records compromised in data breaches by hacktivists, malicious insiders, malicious outsiders and state sponsors, and through accidental loss increased by 86 per cent since 2015, globally.\(^2\) Carbon Black, a cybersecurity company, reported that the dark web marketplace for ransomware has grown at a rate of over 2,500 per cent each year.\(^2\) Among web application attacks,

\(^{21}\) Gemalto, “Breach Level Index 2016”. Available at https://breachlevelindex.com/ (accessed in October 2017). Notes: The data collected has either been reported directly by the company or organization breached, or reported widely by major news outlets. In most cases, there are at least two sources to verify the story. The data for accidental loss accounted for less than 5 per cent of the records.


Notes: During August and September 2017, researchers monitored 21 of the largest dark web marketplaces for new virtual offerings related to ransomware. The description of the offering and sales price was recorded for each offering. To represent the complete dark web economy, the sample of findings from 21 of the largest marketplaces was extrapolated to a population-wide value based on an assumption that approximately 25 per cent of the total dark web website population is composed of similar marketplaces. The analysis was conducted using dark web data dumps of 2016 and 2017 for comparative analysis. The 2016 data dump is available at https://github.com/topics/dark-web, and the deep web data dump is available at https://github.com/vduddu/DeepWebLinks.
Akamai reported that the United States is the largest target. In the Asia-Pacific region, Japan followed by Singapore and India have suffered the highest number of web application attacks during the second quarter of 2017, according to their live monitor of web-based attacks.24

Organizations in certain countries are more likely to experience data breaches. Based on a four-year study by IBM and the Ponemon Institute, South Africa and India have the highest estimated probability of data breach occurrences in the next 24 months, while Germany and Canada have the lowest.25 Arbor Networks26 analysed that enterprises, governments and educational institutes are most concerned with distributed denial-of-service (DDoS) attacks through social engineering and APTs on corporate networks.

According to IBM, the biggest threats in cybersecurity over the past few years have been from phishing attacks, DDoS attacks and malware (especially ransomware). However, CompTia’s 2016 International Trends in CyberSecurity report states that 58 per cent of global firms struggle more with security threats caused by human errors than technology risks, an issue that 61 per cent say has become more of a risk over the past two years.27

The motivations behind these attacks are diverse. Table 1 aims to summarize some of the cyberattack motivations and examples, while Figure 2 illustrates the trends by year and type of security incidents, developed by IBM. Figure 3 shows the number of cyberattacks in Asia-Pacific countries that have been verified by media report between 2013 and 2017, based on data from Gemalto’s Breach Level Index, and Figure 4 shows the number of cyberthreats logged in the third quarter of 2017 in Asia-Pacific countries, based on data from Akamai’s Real-Time Web Monitor.

---

Notes: The collected information came from 1,509 information technology and business executives that were divided into two distinct categories: maturing economies (Brazil, India, Malaysia, Mexico, South Africa, Thailand, and the UAE) and mature economies (Australia, Canada, Germany, Japan, and the United Kingdom). In addition to collecting information by country, the survey covered a variety of job roles, company sizes and industries.
Table 1: Examples of cyberattack motivation categorization

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cybercrime</th>
<th>Hacktivism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Access and propagation</td>
<td>Economic and political advantage</td>
<td>Financial gain</td>
<td>Defamation, press and policy</td>
</tr>
<tr>
<td>Example</td>
<td>Botnets and spam</td>
<td>Advanced persistent threats</td>
<td>Credit card theft</td>
<td>Website defacement</td>
</tr>
</tbody>
</table>

Source: Produced by ESCAP.

Figure 2: Sampling of security incidents by attack type, time and impact (2014-2016)


Notes: Size and type of bubble represent cyberattacks along the timeline identified by IBM and its cybersecurity partners for a particular category. DDoS = distributed denial-of-service; SQLi = structured query language injection; and XSS = cross-site scripting.
**Figure 3: Cyberattacks reported and verified by the media in Asia-Pacific countries (2013-2017)**

<table>
<thead>
<tr>
<th>Country</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>98</td>
</tr>
<tr>
<td>New Zealand</td>
<td>72</td>
</tr>
<tr>
<td>India</td>
<td>59</td>
</tr>
<tr>
<td>Japan</td>
<td>57</td>
</tr>
<tr>
<td>China</td>
<td>38</td>
</tr>
<tr>
<td>Malaysia</td>
<td>33</td>
</tr>
<tr>
<td>Korea (Rep.)</td>
<td>30</td>
</tr>
<tr>
<td>Turkey</td>
<td>21</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>20</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>20</td>
</tr>
<tr>
<td>Pakistan</td>
<td>16</td>
</tr>
<tr>
<td>Singapore</td>
<td>15</td>
</tr>
<tr>
<td>Thailand</td>
<td>11</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>11</td>
</tr>
<tr>
<td>Philippines</td>
<td>9</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>6</td>
</tr>
<tr>
<td>Iran (I.R.)</td>
<td>5</td>
</tr>
<tr>
<td>Cambodia</td>
<td>2</td>
</tr>
<tr>
<td>Myanmar</td>
<td>2</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>1</td>
</tr>
<tr>
<td>Pacific Islands</td>
<td>2</td>
</tr>
<tr>
<td>Central and North Asia</td>
<td>6</td>
</tr>
</tbody>
</table>

Sources: Produced by ESCAP, based on data from Gemalto’s Breach Level Index archives until June 2017. Available at https://breachlevelindex.com/ (accessed in October 2017); and Information is Beautiful: Data Breaches (public). Available at https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iTecxJU2pBKvV6RVRHoYCgIMfg/edit#gid=1 (accessed in September 2017).

Notes: Full archive is available from Gemalto upon request. The number associated with each country represents the number of reported incidents. There may be a reporting bias or data may be incomplete due to translation gaps in countries where reports are in national languages. Only data from ESCAP member countries is considered. Pacific Islands data is based on incidents reported in Samoa and Nauru. Instances of accidental losses and unknown causes are not considered. Reports without a second verifiable source are also omitted, unless the incidents have been self reported by the organization under attack.
**Figure 4: Web-based cyberthreats logged in Asia-Pacific countries (third quarter of 2017)**

<table>
<thead>
<tr>
<th>Country</th>
<th>Threats Logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>1601637</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>327934</td>
</tr>
<tr>
<td>India</td>
<td>222244</td>
</tr>
<tr>
<td>Australia</td>
<td>216541</td>
</tr>
<tr>
<td>Korea (Rep.)</td>
<td>185026</td>
</tr>
<tr>
<td>Japan</td>
<td>160513</td>
</tr>
<tr>
<td>Thailand</td>
<td>159278</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>81617</td>
</tr>
<tr>
<td>New Zealand</td>
<td>74615</td>
</tr>
<tr>
<td>Indonesia</td>
<td>71334</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>66516</td>
</tr>
<tr>
<td>Singapore</td>
<td>54542</td>
</tr>
<tr>
<td>Turkey</td>
<td>44847</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>36864</td>
</tr>
<tr>
<td>Iran (I.R.)</td>
<td>30713</td>
</tr>
<tr>
<td>Malaysia</td>
<td>29856</td>
</tr>
<tr>
<td>Philippines</td>
<td>26957</td>
</tr>
<tr>
<td>Pakistan</td>
<td>24130</td>
</tr>
<tr>
<td>Armenia</td>
<td>14644</td>
</tr>
<tr>
<td>Nepal</td>
<td>11293</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>6721</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>6137</td>
</tr>
<tr>
<td>Cambodia</td>
<td>6098</td>
</tr>
<tr>
<td>Myanmar</td>
<td>2353</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>1970</td>
</tr>
<tr>
<td>Lao P.D.R.</td>
<td>1612</td>
</tr>
<tr>
<td>Georgia</td>
<td>1070</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>1051</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>910</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>841</td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td>585</td>
</tr>
<tr>
<td>Maldives</td>
<td>224</td>
</tr>
<tr>
<td>Fiji</td>
<td>202</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>196</td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>126</td>
</tr>
<tr>
<td>Micronesia</td>
<td>78</td>
</tr>
<tr>
<td>Samoa</td>
<td>28</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>24</td>
</tr>
<tr>
<td>Bhutan</td>
<td>21</td>
</tr>
<tr>
<td>Marshall Islands</td>
<td>17</td>
</tr>
<tr>
<td>Kiribati</td>
<td>13</td>
</tr>
<tr>
<td>Tonga</td>
<td>12</td>
</tr>
<tr>
<td>Vanuatu</td>
<td>4</td>
</tr>
<tr>
<td>Tuvalu</td>
<td>4</td>
</tr>
<tr>
<td>Palau</td>
<td>2</td>
</tr>
<tr>
<td>Nauru</td>
<td>2</td>
</tr>
</tbody>
</table>

Notes: Data presented is as of 8 November 2017. Only data from ESCAP member countries is considered. For the purpose of this graph, cyberthreat is used synonymously with cyberattack. The authors are not clear on what is considered a threat in Akamai’s Real-Time Web Monitor. Attackers may have used virtual private networks (VPNs) to mask the real location of the cyberattack.

2.1 Financial Impact of Cyberattacks

Much has been reported on the financial impact of cyberattacks on organizations and enterprises. Juniper Research claims that cyberattacks resulted in losses of USD 500 billion in 2015, and would quadruple to USD 2.1 trillion by 2019, representing 2.2 per cent of global gross domestic product. Another report by the Centre for International Governance Innovation (CIGI) estimates that cyberattacks resulted in aggregate losses of between USD 5.3 trillion and USD 15.7 trillion in 2016.

The IBM and Ponemon Institute’s study on the cost of data breaches among a sample of 383 companies in 12 countries that had experienced a data breach found that the average total cost of a data breach was USD 4 million in 2017 (up 29 per cent since 2013), and the average cost per lost record was USD 158 in 2017 (up 15 per cent since 2013). Generally, the greatest cost component for organizations is lost business, according to a Kaspersky Labs report. The second greatest is the cost of working with customers and remediation, closely followed by the cost of detection, as highlighted in Figure 5. Figure 6 illustrates cost by type of attack, followed by Figure 7 showing the number of lost records reported between 2013 and 2017 in the Asia-Pacific region.

---


Figure 5: Average financial impact of a data breach


Note: PR = public relations.

Figure 6: Financial impact by type of attack

Figure 7: Number of records reported and verified as lost in Asia-Pacific countries (2013-2017)

Sources: Produced by ESCAP, based on data from Gemalto’s Breach Level Index archives until June 2017. Available at https://breachlevelindex.com/ (accessed in October 2017); and Information is Beautiful: Data Breaches (public). Available at https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iT3RxpU2pBkuV6RVRHoYcLiMfF/edit#gid=1 (accessed in September 2017).

Note: Instances of accidental loss are not considered.

The total number of records reported stolen in 2016 was 1,378,261, out of which the highest number of records lost belonged to government agencies (28 per cent) and the technology industry (28 per cent).
There was also a spike in the number of cross country and global attacks with 1,249,934,495 records reported stolen between 2013 and 2017 in 34 worldwide attacks.⁴⁵

### 2.2 Political Impact of Cyberattacks

There are at least five areas of the electoral process that are potentially vulnerable to hacking. These are: (1) the information received by voters in the lead-up to the election; (2) the rolls used to check voters on election day; (3) the machines on which voters cast their ballots; (4) the tabulation mechanisms for determining the winners; and (5) the dissemination systems used to spread news of the results.⁴⁶ The cyberattacks on political systems affected the way electorates voted in 2017 – some of the reported incidents are found in France,³⁷ the United States of America,³⁸ and Palestine,³⁹ among other countries.

The emergence of AI and social media adds an additional dimension to the cyberattack landscape. For instance, Facebook uses AI to predict users’ actions, and correspondingly, determine the placement of posts and advertisements in users’ newsfeeds that could potentially influence political decisions. The use of AI on social media platforms is also contributing to “viral” posts that are rapidly shared, copied and spread across social media platforms. This phenomenon has become a serious concern as many of these viral posts are not authentic or are created with malicious intent, and as more users get their daily news on social media platforms.⁴²

---

⁴⁵ Based on data from Gemalto’s Breach Level Index archives until June 2017. Available at https://breachlevelindex.com/ (accessed in October 2017); and Information is Beautiful: Data Breaches (public). Available at https://docs.google.com/spreadsheets/d/1Je-YUdnhQJO_13r8ITeRxpU2pBKuV6RVRHoYCiMfg/edit#gid=1 (accessed in September 2017). Note: Instances of accidental loss are not considered.


There are several other ways in which trust in political institutions can be affected. Today, voice, image and video are considered as evidence in the court of law. However, we are at a stage in AI development where these may not necessarily be sufficient anymore. Existing AI-related capabilities include but are not limited to the following:

- Realistically changing the facial expressions and speech-related mouth movements of an individual on video;\(^{43}\)
- Generating a realistic-sounding, synthetic voice recording of any individual for whom there is sufficient training data;\(^{44}\)
- Producing realistic, fake images based only on a text description;\(^{45}\) and
- Producing written news articles based on structured data such as political polls, election results, financial reports and sports game statistics.\(^{46}\)

### 2.3 Related Trends in Cyberattacks

“Smart cities” investing in connecting their infrastructure to the Internet and wirelessly-enabled sensors are more exposed than others. Infrastructure such as water supply, transportation systems and power grids can be attacked remotely. Out of the 60 global metropolises analysed by the Economic Intelligence Unit, cities in Asia (Tokyo, Singapore and Hong Kong) ranked highest in terms of their commitment to digital security, whereas other cities were identified as “not prepared”.\(^{47}\) The World Economic Forum named cyberattacks as the 8th highest risk concern within the next 10 years, and 7th in 2017.\(^{48}\)

According to various reports, large companies experience phishing attacks 57 per cent more often than any other forms of cyberattack.\(^{49}\) Ransomware, botnets and APTs are other areas of great concern and are discussed in the subsections below.

---

2.4 Detailed Analysis by Attack Type

2.4.1 Ransomware

Between 2016 and 2017, the ransomware marketplace grew from USD 250,000 to USD 6 million on the dark web, a growth rate of 2,502 per cent. According to the United States Federal Bureau of Investigation, ransom payments totaled about USD 1 billion in 2016, up from USD 24 million in 2015.50

In Asia-Pacific countries, Internet protocol (IP) addresses registered in the Russian Federation and China have the largest number of ransomware distribution centres. These centres are responsible for distributing ransomware via spam campaigns, social engineering, targeted hacks or exploit kits. They are also leveraging ransomware-as-a-service, which is generally done in a “spray-and-pray” fashion where attackers send the same malicious email to a giant list, hoping a small percentage will click. Businesses are increasingly being targeted, as evident in the WannaCry attacks in 2017.

These findings have been compiled by Ransomwaretracker,51 an open source reporting site that aims to inform cybersecurity professionals about the latest threats in ransomware. However, records from countries located in the Pacific, and Central and North Asia are missing. It is possible that these IP addresses are used as VPNs to deflect the real location of the attackers.

---

Note: Clutch is a business-to-business platform that connects over 7,000 agencies with over 500 digital services. The study surveyed 302 website managers of the private sector who answered questions about cybersecurity measures and types of attacks experienced.


51 Ransomwaretracker is an open source project run by the non-profit organization abuse.ch that identifies botnet command and control, ransomware distribution centres and APTs. Available at https://ransomwaretracker.abuse.ch/tracker/.
Figure 8: Identified IP addresses for ransomware distribution on the Internet (2015-2017)

<table>
<thead>
<tr>
<th>Country</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russian Federation</td>
<td>813</td>
</tr>
<tr>
<td>China</td>
<td>352</td>
</tr>
<tr>
<td>Korea (Rep.)</td>
<td>272</td>
</tr>
<tr>
<td>Turkey</td>
<td>251</td>
</tr>
<tr>
<td>Japan</td>
<td>197</td>
</tr>
<tr>
<td>Thailand</td>
<td>184</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>157</td>
</tr>
<tr>
<td>Australia</td>
<td>137</td>
</tr>
<tr>
<td>Indonesia</td>
<td>109</td>
</tr>
<tr>
<td>Singapore</td>
<td>91</td>
</tr>
<tr>
<td>Malaysia</td>
<td>76</td>
</tr>
<tr>
<td>India</td>
<td>53</td>
</tr>
<tr>
<td>Iran (I.R.)</td>
<td>25</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>11</td>
</tr>
<tr>
<td>New Zealand</td>
<td>8</td>
</tr>
<tr>
<td>Georgia</td>
<td>6</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>3</td>
</tr>
<tr>
<td>Pakistan</td>
<td>3</td>
</tr>
<tr>
<td>Armenia</td>
<td>2</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>2</td>
</tr>
<tr>
<td>Philippines</td>
<td>1</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>1</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>216</td>
</tr>
</tbody>
</table>

Source: Produced by ESCAP, based on data extracted from Ransomwaretracker by tallying the country location of IP address where the attack originated.

Note: It is possible that VPNs were used by the attackers to mask the true source of attack.

2.4.2 Advanced Persistent Threats

With APTs, attackers burrow into networks and maintain "persistence" – a connection that cannot be stopped simply by software updates or rebooting a computer. APTs have been used to attack critical infrastructure, and government or company assets, and are generally well coordinated. An issue with APTs is that they are often not reported publicly by the organization under attack. For example, Yahoo! only

---

53 Paul Szoldra, “These are the most feared hacker groups in the world”, Business Insider, 21 July 2016. Available at https://www.businessinsider.com/advanced-persistent-threats-2016-7/?IR=T.
recently admitted that the cyberattack it experienced in 2013 was much more severe than was originally reported with over 3 billion accounts being breached.\textsuperscript{54}

### 2.4.3 Botnets

Botnets are used for various purposes, as follows:

- Carrying out DDoS attacks by consuming the bandwidth of the victim’s network;
- Spamming;
- Sniffing traffic to retrieve sensitive information like usernames and passwords;
- Keylogging;
- Spreading malware;
- Installing advertisement add-ons as pop-ups on websites;
- Automating clicks on advertisements, thus creating revenue with Google AdSense;
- Attacking Internet Relay Chat networks (similar to a DDoS attack);
- Manipulating online polls and games by casting votes as a real person; and
- Phishing and mass identity theft.

Although bots are used by businesses to automate advertising through search engine optimization, Akamai found that aggressive or poorly-coded bots can overtax the web infrastructure, cause site slowdown and increase latency. The high volume of bot traffic on the Internet, even from good bots, can impose an undesired load on the ICT infrastructure. For many organizations, bots can represent 40-60 per cent of overall site traffic.\textsuperscript{55}

There is a noticeable linkage between the level of bot sophistication and attack duration. DDoS bots use fake-user agents to assume legitimate tool and browser identities in order to avoid detection. The quantity of sophisticated, browser-based bots that retain cookies and execute JavaScript rose from 8 per cent in the third quarter of 2016 to 13.6 per cent in the last quarter of 2016. However in 2017, the number of advanced bots capable of bypassing security countermeasures, i.e., retain cookies and/or execute JavaScript, fell to 2.1 per cent from 9.6 per cent in the first quarter of 2017.

Lately, botnets have been reported to be used for secretly mining cryptocurrency by piggybacking on a vulnerable computer’s processing power to confirm transactions and generate new and potentially

\textsuperscript{54} Laura Hautala, “Your Yahoo account info was definitely hacked – here’s what to do”, \textit{CNET}, 3 October 2017. Available at https://www.cnet.com/how-to/find-out-if-your-yahoo-account-was-hacked/.

lucrative coins.56 Since mining cryptocurrencies require large amounts of central processing unit/graphics processing unit power, the attackers tends to target Windows server machines that are unpatched.57

2.4.4 Phishing

"Phishing" email pretends to be legitimate and asks their intended victims to go online and submit their private information. The fake emails (e.g., fake PayPal or banking-related emails) are generated and sent by bots. Then, social engineering is often used to obtain sensitive information.

Of more than 537,000 phishing threats detected in a study by GreatHorn, 91 per cent contained characteristics of display name spoofs that impersonate a person familiar to an email recipient in order to fool the recipient into thinking that the message is from a trusted source.58 Multiple fake websites pretending to be eBay, PayPal or a bank to harvest personal information have also been identified. Moreover, AI employing social engineering has been used to conduct phishing campaigns.

Other methods of phishing include web server compromise and port redirection. In the former method, attackers break into vulnerable web servers and install malicious web content. They scan for vulnerabilities and when it is found, a rootkit or password-protected backdoor is installed to gain access to the server. In the event that the server is on a cloud, a pre-built website is downloaded. Then, this website is advertised on the Internet through spamming, pay-per-click advertisements, piggybacking or bot traffic. This is done in order to increase visibility of the website for search engines.59 Eventually, web traffic begins arriving at the phishing website and potential victims access malicious content. The Honeynet Project, focused on online security research, found that compromised web servers have also been used as an Internet Relay Chat bot, to scan, locate and attack additional vulnerable computers.60

A port redirection attack is another type of attack based on trust exploitation. This method employs a port-redirection or port-forwarding service installed on a targeted server. The attacker uses a compromised host to gain access through a firewall that would otherwise be blocked. In simple words, every time a computer inside a network wants to connect to a computer on the Internet, it sends the request to the router. This router then takes the connection request and changes it from the private IP of the computer to the public IP of the router, so that the response is sent to the router. Port forwarding is

59 Search engines like Google use website traffic as a major criterion for page ranking.
a way to tell your router what computer inside the network incoming connections should be directed to. Attackers use this method to connect a computer to a compromised server containing malicious content, effectively corrupting a computer. In the analysis by the Honeynet Project, an example of port redirection is the re-routing of Hypertext Transfer Protocol requests sent to a web server to another remote web server, resulting in a phishing attack.

Figure 9: Phishing attacks reported and verified by the online community (2013-2017)


2.4.5 Website Defacement

Website defacement is similar to drawing graffiti on a wall, only it happens virtually. In website defacement, the appearance of the targeted website changes, and pictures and/or words are scrawled across the defaced website. This is the least damaging type of cyberattack carried out but can still lead to bad public relations for a government or company. According to Zone-H’s data archive, out of 30 different hack modes for website defacement during 2014-2015, the most common modes of attack were via structured query language or SQL injection, followed by abusing vulnerabilities in the servers or web applications, and errors made by web administrators. Notably, social engineering and brute force attacks by employing password-guessing AI algorithms were also widely employed (see Figure 10).

Zone H. Available at http://www.zone-h.org.
Note: Zone-H is an open source hack reporting website run by an individual. Its archive with over 18,000 instances from 2012 to 2018 is available upon request. ESCAP has no way of validating the data in the Zone-H archive.
Figure 10: Hack modes for website defacement (2014-2015)

Source: Produced by ESCAP, based on data extracted from Zone-H archives. Available at http://www.zone-h.org (accessed in October 2017).

Notes: Only the top 10 hacks are featured. SQL = structured query language; and URL = uniform resource locator.

Among Asia-Pacific countries, the highest number of website defacement incident was detected in India, followed by the Russian Federation and Indonesia, according to Zone-H archives. However, it is likely that there are more unreported cases.
Figure 11: Website defacement attacks in Asia-Pacific countries (2014-2015)

<table>
<thead>
<tr>
<th>Country</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>2,059</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>1,644</td>
</tr>
<tr>
<td>Indonesia</td>
<td>1,595</td>
</tr>
<tr>
<td>China</td>
<td>1,051</td>
</tr>
<tr>
<td>Australia</td>
<td>750</td>
</tr>
<tr>
<td>Singapore</td>
<td>718</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>619</td>
</tr>
<tr>
<td>Japan</td>
<td>488</td>
</tr>
<tr>
<td>Thailand</td>
<td>418</td>
</tr>
<tr>
<td>Iran (I.R.)</td>
<td>368</td>
</tr>
<tr>
<td>Malaysia</td>
<td>339</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>158</td>
</tr>
<tr>
<td>Korea (Rep.)</td>
<td>148</td>
</tr>
<tr>
<td>New Zealand</td>
<td>79</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>57</td>
</tr>
<tr>
<td>Pakistan</td>
<td>42</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>30</td>
</tr>
<tr>
<td>Georgia</td>
<td>24</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>15</td>
</tr>
<tr>
<td>Philippines</td>
<td>12</td>
</tr>
<tr>
<td>Armenia</td>
<td>8</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>3</td>
</tr>
<tr>
<td>Bhutan</td>
<td>3</td>
</tr>
<tr>
<td>Nepal</td>
<td>3</td>
</tr>
<tr>
<td>Lao P.D.R.</td>
<td>2</td>
</tr>
<tr>
<td>Myanmar</td>
<td>2</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>2</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>2</td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>2</td>
</tr>
<tr>
<td>Maldives</td>
<td>1</td>
</tr>
<tr>
<td>Papua New Guinea</td>
<td>1</td>
</tr>
<tr>
<td>Samoa</td>
<td>1</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Produced by ESCAP, based on data extracted from Zone-H archives. Available at http://www.zone-h.org (accessed in October 2017).
3. Artificial Intelligence in Cyberattacks

Artificial Intelligence (AI) is increasingly used in cyberattacks across the globe. Most machine learning systems have been developed without taking into account possible misuse for cyberattacks, and as a result, the consequences of their misuse are more severe. According to Dr. Dawn Song who explored the relationship between AI and cyberattacks, machine learning systems are often developed to handle confidential data, because sensitive data processing by machine learning eliminates human involvements and errors. However, it is difficult to design defence measures in machine learning that is truly adaptive because of the massive amount of possible inputs. To break a machine learning model, an attacker may compromise its confidentiality, integrity or availability, often referred to as the CIA triad in information security.

Below are some examples of the ways in which AI is being used to design and implement cyberattacks, as follows:

- Self-learning AI systems capable of identifying vulnerable targets, errors in code and network misconfigurations can exacerbate cyberattacks.

- Threat actors can use AI to help calculate and execute attacks designed to do maximum damage, such as carrying out “zero-day exploits”, and even predicting vulnerabilities in future software releases.

- Neural networks can often guess passwords more effectively than state-of-the-art approaches, through methods such as probabilistic context-free grammars and Markov Models, thus allowing attackers to breach password-protected accounts.

- Customizing spear phishing attacks by using AI systems can help gather, organize and process large databases to connect identifying information, making this type of attack easier and faster to carry out. For example, personal information about prospective targets, including details such

---

64 According to Ian Goodfellow, a research scientist at OpenAI (https://www.openai.com/), a non-profit AI research company, and Google Brain (https://ai.google/research/teams/brain), an AI research team at Google.


70 Zero-day exploits refer to vulnerabilities in software, hardware and computer systems that are exploited before a fix becomes available.

71 Markov Models are stochastic models that describe a sequence of possible events in which the probability of each event depends only on the state attained in the previous event. To predict passwords, the observed activities of the system are analysed to infer the probability that the Markov-chain model supports the observed activities.

as where they bank or who their friends are can be identified with AI by analysing publicly available social media profiles and photo accounts.\textsuperscript{73}

- Human Interaction Proofs or CAPTCHAs can be broken by utilizing machine learning to locate the characters (segmentation step) and by employing neural networks for character recognition.\textsuperscript{74}

- Adversarial models capable of tampering with a machine learning model’s integrity can alter its predictions to differ from the intended ones. For instance, spammers can design their email messages to be incorrectly recognized as legitimate messages.\textsuperscript{75}

- Generative models can be used as a compression scheme to reconstruct a different image from the one that the compressor sees.\textsuperscript{76} For example, tricking self-driving cars into seeing a stop sign as a green light resulting in crashes. Generative models can also be used for fraud, for instance, by tricking ATM scanners to read a higher value written on a cheque for withdrawal.\textsuperscript{77}

- An attacker can exploit statistical machine learning to subvert spam filters, as used in the SpamBayes spam filter,\textsuperscript{78} in which a spear phishing attack rendered it useless. The attack was possible even when the attacker only had access to 1 per cent of the machine learning’s training messages.\textsuperscript{79}

---


\textsuperscript{78} SpamBayes is a spam filter that uses statistical machine learning (see http://spambayes.sourceforge.net/). In machine learning, training and testing data are used to verify whether the model used is probabilistically more or less correct in predicting the expected outcomes. In general, the data set is divided randomly into two – one half is used as a training set and the other half as a testing set.

• Attackers can poison training data sets (e.g., poison labels) so that the machine learning system learns the wrong model. The purpose of poisoning attacks may vary from affecting the performance of the learning algorithm to deliberately introducing specific biases in the model.\(^{80}\)

• Attackers, through the use of the model inversion technique, can discover information in the system, including sensitive features used as inputs to decision tree models for lifestyle surveys, and images from application programming interface access to facial recognition services.\(^{81}\)


4. Artificial Intelligence in Cybersecurity

Data science is not traditionally a part of ICT security systems. However, this landscape is changing rapidly as more research is conducted to incorporate AI in cybersecurity. For example, The Defense Advanced Research Projects Agency (DARPA) hosted the Cyber Grand Challenge that set computers against each other in a game to detect, evaluate and patch software vulnerabilities.\(^{82}\)

While the previous section examined the use of AI in cyberattacks, this section looks at machine learning and other aspects of AI in cybersecurity. AI appears to be more useful in passive cybersecurity where the system is capable of assisting cybersecurity professionals in their jobs and preventing data breaches. For example, Cylance is software that uses machine learning to detect and prevent malware from penetrating a network through endpoints. Another example is Darktrace, a company that uses machine learning to learn what is normal for an organization’s network environment to determine abnormal behaviours that can be potential data breaches.

4.1 Machine Learning Applications in Cybersecurity

Machine learning for cybersecurity research has been focused on its direct applications to the open web. Examples include modelling threat propagation for detecting malicious activities,\(^{83}\) adaptive trust modelling for cybersecurity,\(^ {84}\) game-theoretic modelling of cybersecurity threats like information leakage,\(^ {85}\) adaptive attacker strategy evolution,\(^ {86}\) privacy preserving data analysis,\(^ {87}\) attacks on machine learning classifiers,\(^ {88}\) and detecting user authenticity in social networks. Machine learning has also been found to be particularly effective in the areas described in the subsections below.


4.1.1 User and Entity Behaviour Analytics

User and entity behaviour analytics is a machine learning model that discovers security anomalies by: using advanced analysis; aggregating data from logs and reports; and looking at packet, flow, file and other types of information, as well as certain kinds of threat data, to determine the likelihood of a cyberattack. Application log data contains information about user and system action, the networks a system is connected to, the flow of information within a system and between systems, and the condition of a computer system in relation to disk space, errors and audits. AI has the capability to efficiently monitor and go through the huge volume of log data, and pinpoint anomalies in a system.\(^90\)

In particular, machine learning can be used to predict vulnerabilities and modes of attack, and notify a cybersecurity personnel of a network breach. There are at least nine companies that have successfully incorporated machine learning in their cybersecurity products.\(^91\) Recently, Amazon Web Services launched Amazon Macie, a security service that uses machine learning to automatically discover, classify and protect sensitive data.\(^92\) Similarly, a system called App Inventor 2, developed at the Massachusetts Institute of Technology’s Computer Science and Artificial Intelligence Laboratory, reviews data from tens of millions of log lines each day and pinpoints anything suspicious.\(^93\)

4.1.2 Encryption

Cloud applications have improved and proven their reliability over time, with educational and governmental institutions relying on cloud platforms like Citrix management. Cloud applications have become a viable option for enterprises because they are easy to implement and cost less.\(^94\) A key part of secure cloud applications is secure sockets layer/transport layer security (SSL/TLS) encryption. Signified by a Hypertext Transfer Protocol Secure or HTTPS web address and lock icon on browsers, SSL/TLS encryption was primarily developed to provide secure authentication on the web for e-commerce and other financial transactions, but has now expanded its usage into all sectors of web-based security.

The SSL/TLS encryption provides communication security and privacy over the Internet for applications such as web, email, instant messaging and some VPNs. SSL certificates employ cryptography to secure communication between web servers and websites using long strings of randomly generated numbers to


create a key or a password that is only accessible between two endpoints.\textsuperscript{95} Entry into a system’s servers is much more difficult with SSL certification, and thus, a website with SSL certification is more trusted by web browsers. It is also more difficult for attackers to gain entry into an organization’s cloud operations with SSL certification.

However, there have been several cases in which attackers were able to intercept encryption keys and attack a website. Leaked secret keys allow the attacker to decrypt any past and future traffic to the protected services and impersonate the service at will. The OpenSSL Heartbleed vulnerability is one such example.\textsuperscript{96} In response to preventing leaked SSL keys from creating chaos, researchers are focusing on algorithms that continuously rewrite encryption keys, making an enterprise system more secure from attackers trying to access it via endpoints.\textsuperscript{97} For example, researchers from Northwestern University have proposed a methodology called Hamsa, a network-based automated signature generation system for polymorphic worms that is fast, noise-tolerant and attack-resilient.\textsuperscript{98}

### 4.1.3 Deep Learning

Several organizations have “bring your own device” (BYOD) policies, where employees are expected to connect to the organization’s wireless fidelity (Wi-Fi) to work. However, Wi-Fi networks, especially public Wi-Fi networks, are prone to hacking and targeted DDoS attacks. There are several simple tutorials that allow an attacker to access the IP address of a device from a Wi-Fi network and shutdown the system or put ransomware on them. In addition, there are hacking services available on dark web marketplaces, which are elaborated in Section 6.

Wi-Fi devices and networks tend to be less secure than broadband networks. Another issue with BYOD policies is the abuse of organizational information by employees. A report by PricewaterhouseCoopers’ *Global State of Information Security Survey 2015*, found that current employees, previous employees, partners, contractors and customers with malicious intent accounted for the highest share of data


\textsuperscript{97} Ben Rossi, “How AI has created an arms race in the battle against cybercrime”, *Information Age*, 20 March 2017. Available at http://www.information-age.com/ai-created-arms-race-battle-cybercrime-123465117/.

breaches in 2015.\footnote{PricewaterhouseCoopers, \textit{Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015} (2015). Available at \url{https://docs.m0m0g33k.net/CyberSec&GRC/pwc-global-state-of-information-security-survey-20.pdf}. Note: The survey results are based on the responses of more than 9,700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of information technology and security practices across 154 countries. The margin of error is less than 1 per cent.} The 2015 \textit{Data Breach Investigations Report} by Verizon also found that among the insider incidents, 37.6 per cent of the attacks came from ordinary end users.\footnote{Verizon, \textit{2015 Data Breach Investigations Report} (2015). Available at \url{https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf}. Note: Seventy organizations contributed data towards developing this report. All results are based on firsthand evidence collected during paid external forensic investigations and related intelligence operations conducted from 2004 to 2014.}

One way of preventing abuses from insiders is to use AI to monitor employees’ behaviour in a network. AI, through the method of deep learning, can help detect a break from normal employee behaviour, including the discovery of employees that are accessing sensitive company information and transferring this information outside of organization walls. Tasks as harmless as using USB storage can now be analysed for signs of malicious intent and corporate corruption through the help of deep learning algorithms. Deep learning is a machine learning technique that aims to imitate the workings of the human brain in processing data and creating patterns for use in decision-making, allowing the machine to learn unsupervised from data that is unstructured or unlabelled. The use of deep learning to detect instances of policy breaches by employees, however, brings to question the privacy rights of individuals.

**4.1.4 Endpoint Device Security**

Machine learning has also been used to secure endpoint devices such as mobile phones, iPads and notebooks. Thirty per cent of Android users do not protect their smartphones with passwords, and 44 per cent do not have an anti-malware solution installed, according to research from Kaspersky Labs and B2B International.\footnote{Alan Zeichick, “The IoT calls for an AI-based security approach”, \textit{Network World}, 14 December 2015. Available at \url{https://www.networkworld.com/article/3014499/internet-of-things/the-iot-calls-for-an-ai-based-security-approach.html}. Note: During 2013 and 2014, Kaspersky Lab detected around 315,000 daily malicious samples.} However, applications such as Zimperium can be used to distinguish normal from malicious behaviour on Android and iOS devices. It uses the z9 engine that is inserted into a device within the zIPS app, which is capable of performing device and network forensics, and detecting malware. It provides the device user with information on nearby Wi-Fi networks and their potential risks, and alerts the user if a network is vulnerable to attackers and hackers. The application also compiles this data and notifies other users in the zIPS network of the Wi-Fi risks.

Additionally, endpoint device security through apps like these that employ machine learning allows enterprise-level mobile device security solutions, and can help ensure that enterprise network security policies are upheld. With the possibility of monitoring mobile devices within a workplace, BYOD policies become more resilient. However, these devices may also contain personal information and data. While
endpoint device security is important and machine learning is making it increasingly easy to monitor these devices, enterprises having access to an employee’s personal data may be interpreted as surveillance and further privacy policy discussion needs to be conducted on this matter.

4.1.5 Risk Modelling

Defensive capabilities include preparation, prevention, detection, response and recovery against cyberattack, which could be enhanced with machine learning models. With respect to detection, several machine learning models are available to help visualize large quantities of logged data and present it in a comprehensible way. Some examples include:

- Algorithms that employ natural language processing to produce documentation containing repetitive tests and charts to intelligently describe analysis of application logs, packets, etc.;
- Automation and open source coding to streamline risk modelling data collection, cleaning, validation and calculation;
- Automated clustering applications to visualize and speed up the process of cybersecurity analysis using tools such as Graphistry; and
- Robotic process automation and mixed data processing architecture that can lower cybersecurity costs and improve efficiency in threat detection.

4.1.6 Honeypots

Honeypots are designed to lure attackers by masquerading as a web server, pretending to contain the kind of personal data that attackers are looking for, such as credit card numbers, emails and medical records. AI programs are able to learn the behaviour of thousands of bots in cyberspace and group them into networks based on that behaviour.

In September and October 2016, attackers leveraged hundreds of thousands of IoT devices with weak telnet passwords to launch DDoS attacks. An analysis by Arbor Networks on the Mirai botnet using

---


honeypots found that the top three countries with the most number of attacks are in the Asia-Pacific region (see Table 2).

Table 2: Top five IP addresses with Mirai Botnet collected by honeypots

<table>
<thead>
<tr>
<th>Country</th>
<th>No. of Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>102,975</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>15,573</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>29,465</td>
</tr>
<tr>
<td>United States of America</td>
<td>17,062</td>
</tr>
<tr>
<td>Brazil</td>
<td>16,609</td>
</tr>
</tbody>
</table>


4.2 Limitations of Machine Learning

Since machine learning “learns” from past behaviours, any previously unseen attacker is to some extent invisible to machine learning algorithms because there is no prior history from which to learn. Essentially, the AI community is still working on handling cybersecurity from various angles but there may not necessarily be a machine learning approach that can handle issues such as credential spear phishing where there are too few known anomalies in any given data set from which the algorithm can successfully learn. For enterprises that are looking to use machine learning for cybersecurity, it is important to have an enterprise logging policy and ensure that logs are aggregated and analysed in a useful way.106

---

5. Internet of Things Security

An integral part of AI is IoT, which connects devices to machines to collect and transmit data that is in many cases used for Big Data analytics and machine learning. IoT has been instrumental in improving efficiencies and data availability in monitoring weather, conditions of building and infrastructure, and movements of goods and medical supplies, to name a few areas.

Juniper Research reported that the number of IoT connected devices will grow to 38.5 billion in 2020, up from 13.4 billion in 2015 – representing a rise of over 285 per cent. Along similar lines, the McKinsey Global Institute predicts that the total potential economic impact of IoT will be in the range of USD 3.9 trillion to USD 11.1 trillion per year in 2025. However, because of the ubiquitous nature of IoT, the associated cyberrisks could also increase exponentially, and significantly affect people’s homes, offices, schools and hospitals through smart homes, smart television, smart cars and smart grid applications.

IoT devices have access to and can be accessed by outside parties such as cloud and mobile services. Companies like Salesforce have advertised AI products, such as Einstein, for troubleshooting and customer services through remote monitoring of IoT. They detail how a dishwasher connected to the Salesforce IoT Cloud is capable of identifying issues and dispatching a repair technician without the customer or agent being involved. Such connectivity could present a threat to device security.

In recent years, attacks on IoT have focused on critical infrastructure. For example, hackers attacked a German steel mill in 2015, and in the same year, shut down a Ukrainian power station resulting in 80,000 people losing power. In another case, two cybersecurity experts demonstrated how they took control over a jeep as it was cruising down the highway. IoT devices continue to be compromised on a massive scale and are used to mount DDoS attacks that are disrupting companies. Cybercriminals have

110 Kim Zetter, “A cyberattack has caused confirmed physical damage for the second time ever”, Wired, 8 January 2015. Available at https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
also found new ways to compromise Android devices using overlay attacks, despite operating system security updates.\textsuperscript{113}

\subsection*{5.1 Machine Learning in IoT Security}

The machine learning community has responded to the security challenges of multiple connected devices that need to be monitored with quick large-scale monitoring capabilities. For instance, network-based solutions can help secure IoT devices by defining and registering every device that is allowed to access a network in order to prevent intruders from hacking into IoT networks. Machine learning engines that monitor incoming and outgoing IoT device traffic can then create a profile that determines the normal behaviour of the IoT ecosystem. From there, detecting threats involve discovering traffic and exchanges that do not fall within the established normal behaviour. This is similar to the above-mentioned user and entity behaviour analytics (Section 4.1.1) to alert device owners about potential risks and suspicious behaviour.

In practice, the functionality of each IoT device is very limited, and thus, it is much harder to sneak in malicious requests and much easier to establish a finite set of rules to determine normal and anomalous behaviour. These traffic monitoring schemes can also be applied to interactions between devices, resulting in finding attacks from compromised devices. Even though IoT has a large number of logs with respect to machine-to-machine traffic, the limited functionality and interaction of each device means that singling out devices that are engaging in abnormal exchanges with other devices in the network is relatively easy.

Most IoT devices come equipped with signature-based protection, but cryptography has been proven to be inefficient for the protection of IoT since most users generally do not change the password that comes with the device. This inefficiency can, however, be compensated by behaviour-based solutions. Other machine learning-based solutions include honeypotting. For example, the HoneyThing Project\textsuperscript{114} is a honeypot for Internet of TR-069 Things, which is designed to act as a modem/router that has RomPager embedded web server and supports the TR-069 (CWMP) protocol.\textsuperscript{115}


\textsuperscript{114} Omer Erdem, “HoneyThing Project”. Available at https://github.com/omererdem/honeything.

6. The Dark Web Marketplace

The dark web is an encrypted portion of the Internet that is not indexed by search engines. Access to dark web pages requires special software with the correct decryption key, as well as access rights and knowledge of where to find the content. While the dark web is often portrayed as a domain for illegal activities such as drug sales and child pornography, the dark web also enables anonymous whistleblowing and protects users from surveillance and censorship.

Table 3: Price range of hacked accounts on the dark web

<table>
<thead>
<tr>
<th>Service</th>
<th>Minimum Price (USD)</th>
<th>Maximum Price (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>0.70</td>
<td>1.20</td>
</tr>
<tr>
<td>Gmail</td>
<td>0.70</td>
<td>1.20</td>
</tr>
<tr>
<td>Dell</td>
<td>0.80</td>
<td>2</td>
</tr>
<tr>
<td>Uber</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Amazon</td>
<td>0.70</td>
<td>6</td>
</tr>
<tr>
<td>Paypal</td>
<td>1</td>
<td>80</td>
</tr>
</tbody>
</table>


The dark web marketplace expands to providing goods and services for conducting cyberattacks. Today, it is just as easy to buy code packages for hacking into servers and systems as it is to buy bulk email, Instagram and Pinterest accounts for black hat search engine optimization and phishing. For example, users can buy government email lists to conduct cyberespionage.

Phishing-as-a-service is a store on the Russian dark web that offers a complete solution for a novice scammer, which includes the scam page, the landing page and a backend database to store the stolen credentials. An SMTP server is sold on the dark web for between USD 1.25 and USD 3, while a list of

---

100,000 emails costs between USD 2 and USD 50, depending on the country or type of emails, and their "freshness" or the length of time since they were stolen.\textsuperscript{121}

Figure 12 illustrates the number of instances by cyberattack goods category, followed by Figure 13 on the average costs for cyberattack services on the dark web, and Figure 14 on the number of vendors offering various cyberattack services on the dark web.

\textbf{Figure 12: Number of instances by category in the dark web marketplace}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure12.png}
\caption{Number of instances by category in the dark web marketplace.}
\end{figure}


Figure 13: Average cost requested for cyberattack services on the dark web marketplace


Figure 14: Number of vendors offering cyberattack services in the dark web marketplace

7. The Way Forward

The sections above highlighted cyberattack and cybersecurity trends based on data and reports available. Emanating from the narratives are some key cybersecurity issues that have had a significant impact on societies and economies. As AI and other emerging technologies are still evolving, relevant policies, regulations, laws and legislations may not be in place or fully updated to address the various issues and challenges they present. Nonetheless, in light of the issues that have surfaced, this section offers some recommended actions for the way forward. The list below is not meant to be exhaustive. As technologies mature and evolve, additional perspectives or new issues are expected to emerge.

1. **Ensure the privacy of individuals**: In the age of Big Data, the massive amounts of data generated and collected, sold and traded by third parties are a worrying trend globally. With AI, businesses can analyse more complex data and get more accurate results. Today, online services and smart devices are constantly collecting users’ data, including sites visited, purchases made, geolocation, Wi-Fi network information, voice and image recordings, and other personal details, thus potentially reducing users’ privacy and safety. Similarly, using tracking AI in business networks capable of monitoring emails, documents and photographs of employees and their activities in the network is a sensitive topic. Employees should be trained and informed about company practices collecting personal data and the use of such data. To track the extent to which countries are safeguarding their citizens’ privacy rights, a global cyberprivacy index could be developed.

2. **Establish an incident reporting mechanism**: This includes monitoring and assessing the occurrences of cyberattacks and data breaches, including their nature, scope and impact, as well as details of the responses to incidents. One of the challenges government officials may encounter is obtaining an accurate picture of the cyberrisks without an incident reporting mechanism. When Australia and New Zealand established a government audit process, there were 44 and 16 voluntarily reported data breaches in the respective countries. With the new Privacy Amendment (Notifiable Data Breaches) Act 2017 in Australia, the numbers are expected to increase dramatically as organizations are required to declare any “eligible data breaches”.

3. **Strengthen laws and legislations, and increase penalties for cyberattackers and hackers**: There is no international framework that binds countries in terms of offensive cyberoperations, but some countries have started initiating the establishment of national laws and legislations to define responsibilities, increase penalties for various cybercrimes, and ensure citizens’ safety and security.

4. **Plan and implement digital safety and digital literacy initiatives**: These initiatives could be supported by developing and updating cybersecurity policies in the private sector and government organizations, organizing training and awareness campaigns, and creating methods for measuring employees’ compliance to cybersecurity standards and policies. It would be important to develop digital safety and
digital literacy indicators to better gauge the current state of cybersecurity awareness among individuals and organizations worldwide.

5. **Invest in cybersecurity research and initiatives**: One of the common challenges faced by governments in the region is securing sufficient funding and investments to address cybersecurity. The increasing level of sophistication in cyberattacks would require government officials to upgrade their cybersecurity knowledge and skills on a regular basis. Regional cooperation and knowledge sharing would also be crucial for addressing the wide range of cyberthreats and risks.

6. **Promote cybersecurity best practices for individuals and organizations**: Although not exhaustive, some of the cybersecurity best practices for individual users include the following:

- **Clear cache in browsers and devices** – This involves clearing browsing history, and removing stored passwords and related information. Clearing a browser’s cache makes it more difficult for attackers to access personal information such as email passwords and bank account information. It is also important to change passwords regularly.

- **Update software regularly** – Several hacks have been carried out by exploiting software vulnerabilities. Attackers exploit this weakness by writing codes to target a specific vulnerability. Software and system updates generally involve patching vulnerabilities, and improving operation system’s functionality and performance.

- **Enable two-factor authentication for account log in**\(^{124}\) – To deter password-guessing attacks, two-factor authentication can be helpful. With two-factor authentication, attackers will have to either acquire the physical component of the log in, or gain access to the cookies or tokens placed on the device by the authentication mechanism. Various account services such as Facebook, Google and online banking services offer two-factor authentication, and it is highly encouraged.\(^{125}\)

- **Know your right to privacy** – The Cookie Law is a privacy legislation in Europe that requires websites to obtain consent from visitors to store or retrieve any information on a computer, smartphone or tablet.\(^{126}\) Individuals have the right to refuse the use of cookies to track browsing history. In addition, review privacy policies and adjust privacy settings of the sites used, particularly, social media sites.

- **Do not automatically connect to Wi-Fi networks and store Wi-Fi passwords** – As discussed above, public Wi-Fi networks are vulnerable to hacks and pose security risks.

---


\(^{125}\) List of companies offering two-factor authentication. Available at https://twofactorauth.org/.

\(^{126}\) OneTrust, "The Cookie Law Explained". Available at https://www.cookielaw.org/the-cookie-law/.
• Use VPNs to hide the actual IP address – However, this method may not be applicable in certain Asia-Pacific countries and should be used following the regulations in specific countries.
Annex A: Glossary

1. **Cyberattack**: Actions performed by non-state actors to undermine the function of a computer network and violate criminal law, and may or may not have a political or national security purpose.\textsuperscript{127}

2. **Cyberwarfare**: Actions by nation states or international organizations to attack and attempt to damage another nation’s computers or information networks, especially for political or military purposes.\textsuperscript{128}

3. **Cybersecurity**: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment, organizations and users’ assets.\textsuperscript{129}

4. **Active Cyberdefence**: Synchronized, real-time capability to discover, detect, analyse and mitigate threats and vulnerabilities using sensors, software and intelligence.\textsuperscript{130}

5. **Passive Cyberdefence**: Measure for detecting and mitigating cyberintrusions and the effects of cyberattacks that does not involve launching a preventive, pre-emptive or countering operation against the source (e.g., firewalls, patches, antivirus software and digital forensics tools).

6. **Endpoint**: Devices connecting to an enterprise network. Any device, such as a smartphone, tablet or laptop, provides an entry point for threats.

7. **Internet of Things**: A global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communications technologies.\textsuperscript{131}


\textsuperscript{128} RAND, “Cyber Warfare”. Available at https://www.rand.org/topics/cyber-warfare.html; and TechTarget, “Cyberwarfare”. Available at https://searchsecurity.techtarget.com/definition/cyberwarfare.


8. **Artificial Intelligence**: The mechanical simulation system of collecting knowledge and information, and processing intelligence of universe: (collating and interpreting) and disseminating it to the eligible in the form of actionable intelligence.\(^{132}\)

9. **Machine Learning**: A type of artificial intelligence that allows software applications to become more accurate in predicting outcomes by automatically learning and improving from experience.\(^{133}\)

10. **Data Mining**: A broad set of techniques and algorithms for extracting useful patterns and models from very large data sets.\(^{134}\)

11. **Server**: A computer designed to process requests and deliver data to other (client) computers over a local network or the Internet.\(^{135}\)

12. **Web Server**: A computer that stores a website's component files (e.g., HTML documents, images, CSS stylesheets, and JavaScript files), delivers them to the end-user's device and controls how web users access hosted files, at minimum a Hypertext Transfer Protocol server.\(^{136}\)

13. **Rootkit**: A clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence.\(^{137}\)

14. **Pay per Click**: A way of using search engine advertising (such as Google AdWords) to generate clicks to a website.\(^{138}\)

15. **Internet Relay Chat**: A protocol that facilitates communication in the form of text working on a client/server networking model to transfer messages to other clients.\(^{139}\)

16. **Piggybacking**: The practice of establishing a wireless Internet connection by using another subscriber's wireless service without the subscriber's explicit permission or knowledge.


17. **Honeypot**: A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

18. **Malware**: Short for malicious software, it is software that is used to disrupt computer operation, gather sensitive information or gain access to private computer systems. Types of malware include ransomware, adware, scareware and spyware.

19. **Ransomware**: A subset of malware in which data on a victim’s computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.

20. **Spyware/Keylogger**: A type of surveillance software that once installed on a system, has the capability to record every keystroke made on that system. A keylogger can record instant messages, email, and capture any information typed at any time using the keyboard connected to the compromised system, including usernames, passwords and other personally identifiable information.

21. **Phishing**: A cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

22. **Spear Phishing**: An email or electronic communications scam targeted towards a specific individual, organization or business intended to steal data for malicious purposes, cybercriminals or to install malware on a targeted user’s computer.

23. **Advanced Persistent Threat**: A network attack in which an unauthorized person gains access to a network in order to steal data by using multiple phases to break into a network, avoid detection and harvest valuable information over the long term.

24. **Social Engineering**: The art of manipulating people so they give up confidential information such as passwords or bank information, or to secretly install malicious software that gives control over a computer.

---

25. **Bot**: A bot, or web robot, is a software application that runs automated tasks over the Internet. Bots may be deployed by search engines, competitors and other third parties to capture data and information from websites.\(^{147}\)

26. **Botnet**: A collection of Internet-connected user computers (bots) infected by malicious software that allows the computers to be controlled remotely by an operator through a command-and-control server to perform automated tasks, such as stealing information or launching attacks on other computers.\(^{148}\)

27. **Application Layer Attack**: An attack that targets the vulnerabilities in the structural code of applications. An example is bringing down a server by exhausting its processing resources (i.e., central processing unit or random-access memory) with a high number of requests.

28. **Network Layer Attack**: An attack against either the network or transport layer that causes network saturation by expending available bandwidth.

29. **Brute Force Attack**: Consists of an attacker trying many passwords with the hope of eventually guessing correctly.\(^{149}\)

30. **Distributed Denial-of-Service Attack**: A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. It utilizes multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.\(^{150}\)

---


\(^{150}\) Cloudflare, "What is a DDoS Attack?" Available at https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.
Annex B: Broadband Connectivity is a Requirement for Cybersecurity

As discussed in a publication of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) entitled, State of ICT Connectivity in Asia and the Pacific 2017,\(^{151}\) the advent and proliferation of the “Fourth Industrial Revolution” technologies, namely Artificial Intelligence (AI), the Internet of Things, Big Data analytics and automated systems, are not possible without the three tiers of core infrastructure: secure, reliable and resilient **fixed broadband connectivity**, **data centres** and **cloud computing**.

The benefits of AI and related technologies cannot be enjoyed by countries that are lagging behind in digital integration. Among ESCAP member states, the digital divide is growing rapidly between countries that are quick in broadband investment and uptake, and countries that are struggling to adapt to the digital era. ESCAP reported that the digital divide is especially wide in small island developing states such as the Pacific Islands, landlocked developing states in Central and North Asia and least developing countries.

The number of cybersecurity breaches amongst government agencies, educational institutions and the private sector has seen a significant increase in recent years. The United States of America, for instance, observed a growth in cyberattacks from 2006 to 2012. In 2017, almost half of all British firms were hit by cyberbreaches or attacks.\(^{153}\) The rise in cyberattacks can be attributed to advancement in predictive analysis and behaviour replication algorithms in AI, and a lax attitude towards cybersecurity policy that allows cybercriminals to exploit vulnerabilities in cyberspace.

The most common breaches or attacks were via fraudulent emails that coax staff into revealing passwords or financial information, or opening dangerous attachments. This is followed by attacks using viruses and malware, including ransomware. WannaCry, a global ransomware attack on government agencies and financial institutions in 2017 was perpetrated using AI technology in exchange for bitcoin.

In terms of cybersecurity, fixed broadband connections and server systems are more secure than mobile broadband systems. Mobile broadband is not a secure connection for institutional and government agencies. In Europe, although security breaches, attacks and hacks of mobile broadband systems reported in 2012 decreased from the previous year, it was still significantly less secure than fixed broadband platforms.

---


A major challenge in mobile phone communications is that the network operator is the unknown third party in the communication chain. Since network operators have to generally communicate with regional partners for data to be transmitted to a foreign country, more than one mobile phone service provider is almost always involved.\textsuperscript{155} Security experts have voiced their concern over the vulnerabilities in 4G networks that only use IP architecture.\textsuperscript{156}

Similarly, with wireless traffic it is easy for attackers to disrupt businesses by launching wireless packet floods against access points, nearby servers, next-hop wired network or Internet uplink. This is because wireless traffic is easily recorded, which allows intruders to steal Internet bandwidth, transmit spam or use the network to attack others.\textsuperscript{157}

