K. Thakur et al., *Emerging ICT Technologies and Cybersecurity*
https://doi.org/10.1007/978-3-031-27765-8_11

# 11. Impact of Advanced and Futuristic Technologies on Cybersecurity

Kutub Thakur[1] ✉, Al-Sakib Khan Pathan[2] ✉ and Sadia Ismat[3] ✉

(1) Department of Professional Security Studies, New Jersey City University, Jersey City, NJ, USA

(2) Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh

(3) Department of Professional Security Studies, New Jersey City University, Jersey City, NJ, USA

✉ **Kutub Thakur (Corresponding author)**
**Email:** kthakur@njcu.edu

✉ **Al-Sakib Khan Pathan**
**Email:** sakib.pathan@gmail.com

✉ **Sadia Ismat**
**Email:** sismat@njcu.edu

## Overview of Impact of Modern Technologies on Cybersecurity

The threat surface expands with the expansion and utilization of more technologies and technological ecosystems because the new technologies that are evolving are used in the business much faster to achieve the competitive-edge in the market and to capture as much share of the market as possible. This race of capturing more markets with the help of advanced and emerging technologies often leave numerous security aspects skipped and overlooked. The hackers exploit the possible vulnerabilities and overlooked loopholes in the security of the software applications to hack into the security system and unleash cyber-attacks on a vast threat surface.

How does threat surface expand with the usage of advanced and emerging technologies? There are many aspects of using emerging technologies that can expand the threat surface. A few of those contributing factors include [281]:

- Emerging technologies have not got fully matured because technologies keep evolving with cybersecurity loopholes and then, exploitation from the hackers is noticed. Thus, at the starting point the cybersecurity threat landscape increases significantly due to those numerous security loopholes in different parts of the software and associated firmware.
- The number of intrusion points increase, which provides the hackers a large landscape of opportunities to intrude into the security systems. For instance, the number of devices connected under the technology stack of Internet of Things (IoT) is in billions. All those devices use different types of firmware, software, communication protocols, and security mechanism. That provides a much larger area for hackers to exploit any vulnerability in the codes and mechanisms of those devices to get information about the other connected networks and devices for launching cyberattacks.
- Operations and maintenance of a large number of devices connected under the umbrella of emerging technologies becomes so difficult. The upgradation, malfunctioning, removal of any malicious code installed on those devices and technologies points become very difficult due to numerous factors. This increases the opportunities for cyber threat actors to attack the security systems of the technological landscape.
- The use of weak communication protocols such as signaling system 7 (SS7) and a few older systems that are still in use in many devices for communication increase the threat levels in the modern cybersecurity systems powered by the latest technologies.
- The operators of new technologies or the end-users (who are normally not expert users) incur troubles. The general users are often not the trained users who are aware of the risk factors associated with the newer technologies. They mostly fall prey to the hackers through numerous ways such as social engineering, password management, and service/product using behaviors.
- Compatibility and interoperability issues also increase with the deployment of modern and emerging technologies with the existing technological ecosystem. Different standards and operational guidelines may not be compatible with the other systems that create

a disharmony and loopholes in the comprehensiveness of the cybersecurity of systems.
- Advanced skills and expertise of hackers who always try to explore the possible vulnerabilities in the emerging technologies often hit the markets. They are highly specialized and sophisticated people to figure out the possible chances of breaking the security of the newly introduced technologies. This also increases the threat landscape substantially.
- The usage of advanced hacking tools such as botnets, network mapper (Nmap), Nessus, NetStumbler and many others powered by the modern technologies such as extended reality, machine learning, artificial intelligence and, any other mechanism make the new products and services more prone to the data breaches and other anomalies.
- The extended use of social media is also increasing the risk of cyber-threats because modern software that can analyze the user behaviors and their interests and their working patterns can convert them into different traps and use those patterns for hacking purposes.

Thus, the threat space expands with the usage of newer technologies and bigger networks. Finding the security experts or operations and management specialists for the newer or emerging technologies is often an uphill task. This also leads to expansion of threat landscape in the cybersecurity. Thus, the expanding threats landscape in the technological ecosystems powered by the modern/advanced technologies can be reduced or averted in certain cases by using the following techniques and schemes in the cybersecurity systems [282, 283]:

- Continual monitoring and updating of the software and hardware tools used in the networks through automated as well as manual schemes.
- Training the company staff as well as the users for maintaining as much security as possible to reduce the risk of cyberattacks.
- Use advanced technologies in communication such as transmission and cloud encryption for data storage and transportation.
- Usage of highly secure technologies in cybersecurity systems such as blockchain, artificial intelligence, machine learning, and others.

- Deploy behavior analytics powered by big data and AI analytics.
- Incorporation of context-aware security for making data driven decisions regarding the emerging threats in real-time environment.
- Implementation of defensive artificial intelligence (AI) powered tools for preemptive measures before the cyberattack can hit the assets.
- Deployment of Manufacturer Usage Description (MUD) standard for the security of IoT devices. This standard is built by the Internet Engineering Task Force (IETF) for home and SMB (Small and Midsize Business) automation.
- Incorporate the Extended Detection and Response (XDR) systems for preventing any emerging intrusion from the hackers.
- Adopt zero-trust or never-trust and always-verify policy in your company, partners, and stakeholders simultaneously. Deploying an architectural framework named as Zero Trust eXtended (ZTX) is the best option to implement this policy.
- Avoid using the faulty protocols in your communication systems such as SS7, Diameter, Session Initiation Protocol (SIP) and others that have already been exploited by the malicious actors in the cybersecurity field.
- Implement server-less cloud and container ecosystem for more robust cybersecurity in your system to prevent malicious intrusion or data breaches.

With the advancements in the technologies, the threat landscape increases in cybersecurity; at the same time, it offers numerous solutions to overcome the emerging cybersecurity challenges in the modern IT world.

---

## Major Cybersecurity Challenges Due to Advanced Technologies

According to the Strategic Market Research forecast, the global cybersecurity market is expected to reach a whopping USD $478.68 billion by 2030 due to huge impact of the emerging and disruptive technologies that have already shown their impact on the industries across all domains. The global market of cybersecurity in 2021 was measured as much as USD $216.10 billion. This huge or exponential growth in the global market size of cybersecurity was estimated at about 9.5% CAGR during the forecast period [284]. The main technologies that have increased the landscape of cybersecurity threats include bring your own device (BYOD) standards and IoT technology ecosystem. Other emerging technologies that have also empowered the hackers and malicious users include artificial intelligence (AI), machine learning (ML), data analytics, big data, natural language processing (NLP), and many others.

The impact of those technologies is felt in numerous day-to-day personal, business, and governmental activities. For instance, the total cost of cybercrimes in the world is expected to cross USD $10.5 trillion annually, which were just USD $6 trillion in 2021 [285]. Looking at this staggering figure, everyone can understand the gravity of the cybersecurity threat to the businesses across all domains and industries in the world. The average growth in the global losses to the business world due to cybercrimes is expected to remain above 15% year over year for the projected time period.

There are domains other than business world that face serious challenges or threats due to the cybersecurity issues emerging through the newly introduced technologies and those futuristic technologies that are expected to hit the markets very soon. The strongest impact of cybersecurity due to the emerging technologies is especially noticed in the following domains:

- Risk to National Security
- Breach of Privacy
- Increased Burden of Cybersecurity on Businesses
- Shortage of Cybersecurity Specialists
- Risk of Extensive Data Exposure
- Society and Business Manipulation.

Let us now separately explore the above-mentioned domains where the impact of cybersecurity due to the emerging technologies is felt significantly.

## Risk to National Security

Some quality research works on the impact of cyber threats on the national security suggest that cybersecurity threat not only impacts the businesses and people living in a country but also the national security of that particular country in different forms and manifestation. Today's world is so connected and interlinked that nobody can escape the impact of one thing in a country or even in a foreign country in terms of numerous factors. The impact can be divided into two separate categories—(1) that, which is inflicted on a nation as direct cyberattack on the security institutes, agencies, and their assets—(2) that in which the entire ecosystem of a nation is disturbed, which results into chaos and internal disturbances.

The main impacts of a cybersecurity that can lead to national security issues include the following [286]:

- Loss to major businesses that contribute significantly to the economic development and stability of a nation.
- Stealing and manipulation of data of the common people and target them for the activities that can be detrimental and destructive for the country's security.
- Creating panic and social disturbances through different means when the data of the most vulnerable sections of the society is available for exploitation.
- Stirring political chaotic conditions based on the sensitive data and information collected through data breaches and cybersecurity attacks.
- Tearing the social fabric and community harmony in any country for destabilizing the economic, political, and social activities.

The other impact of cybersecurity on the national security may be very direct, in which the cyberattacks are launched on the data, secrets, systems, assets, plans to steal and misappropriate them in accordance with the needs of the adversary that wants to inflict damages to the national security a particular country in certain conditions. Another direct impact can be the cyberattacks on the utilities and other civic services so that the chaotic conditions are created in a country to carry out the most dangerous designs and activities by exploiting those conditions.

The innovative and emerging technologies add fuel to this impact because those technologies are released early (than the time of maturity) and often to establish competitive-edge by compromising the impact of the cybersecurity on the businesses, national security, and the people of the country. Thus, a serious warning should be taken by the concerned businesses, governments, institutes, and people about the impact of the cybersecurity on the national security, which is the most fundamental component for running governments, businesses, and societies smoothly.

Indeed, the threats to the states and communities exist through the cyberspace. Therefore, cybersecurity should always be treated from the national security perspective and standpoints.

## Breach of Privacy

According to the latest information, the total number of people that were affected in breach of privacy impact in the US only was 53.35 million in just first quarter of the 2022. With this figure, it is not very difficult to imagine about the impact of data breach on the people across the globe [287]. Almost, every Internet-connected or online person has shouldered the impact of privacy breach in one way or the other. The breach of privacy keeps increasing with the emergence of the modern technologies due to the same reasons such as:

- Over excitement of the users to use the newer technologies without knowing or taking care of the impact of those technologies on privacy breaches.
- Early release of products or services based on the innovative technologies by the companies while ignoring the privacy breach issues.
- Unavailability of domain expertise and security professionals to deal with the emerging data breach threats.

## Increased Burden of Cybersecurity on Businesses

The scale of damages caused by the cybersecurity threats in the world is huge in trillions a year. To avert or reduce the impact of that huge devastation, businesses focus on investing hugely on the cybersecurity to maintain a robust and reliable security level to avoid any kinds of damages caused by the cyber attacks. The average annualized spending by the businesses in the cybersecurity field is expected to cross USD $1.75 trillion by 2025 [288].

This huge burden is increasing very fast due to the emergence of the most advanced and latest technologies and innovative platforms. Thus, the businesses are badly impacted with the burden of such as huge amount of money, which is spent on the maintenance and enhancement of the cybersecurity systems and professionals.

## Shortage of Cybersecurity Specialists

Another impact of emerging technologies is the shortage of the cybersecurity professionals. Entire world has already been walking through tough time due to the shortage of skilled and qualified cybersecurity professionals. The advancements in the emerging technologies and newly introduced technological business ecosystems have aggregated this problem for all types of businesses and government agencies simultaneously.

According to the latest estimation by World Economic Forum, there is a huge shortage of cybersecurity professionals in the world. There are about 3,000,000 experts and specialists short of the requirements in this field. This demand is continuously increasing and the availability of the cybersecurity professionals is continuously depleting. Thus, the impact of modern technologies on different entities—business and governmental—is the shortage of cybersecurity professionals, experts, and specialists [289].

## Risk of Extensive Data Exposure

The most competitive business environment is where gaining competitive-edge through different innovative ways is the only way for the companies and organizations. In such environment where the hackers and malicious actors are more organized and bold to attack and there is a huge shortage of cybersecurity professionals to counter them, the chances of extensive data exposure will remain very high. With the excitement of newer technologies among both the users and providers, the situation is becoming more precarious for extensive data exposures and data breaches.

The main reasons of data exposures pertaining to modern and innovative technologies include the following:

- Use of huge number of devices in highly diverse environments of IoT where a large number of devices run diverse firmware and software.

- Increased number of user accounts with those huge number of devices and related services are also prone to data exposure.
- Mismanagement in password creation, maintenance, and storage by the clients.
- Outdated software and devices that are not updated regular also exaggerate the situation.
- Continual emergence of innovative techniques and ways that people are not fully expert at.

## Society and Business Manipulation

Another impact of the modern and emerging technologies on the cybersecurity is that by breaching the control of cybersecurity or through other means, the entire society of a country or a business ecosystem of a nation can be manipulated and streamlined for the benefit of the adversary. This can be done through the most modern and innovative technological approaches to analyze the behaviors and activities of the people and businesses in a particular field or industry and achieve the most actionable data that the people and businesses are influenced with.

The examples of such incidence were reported in the US presidential elections in 2016. In those elections, it is alleged that Russia tried to manipulate the mandate in favor of a particular party by building an opinion in the people in such a way that they would be easily influenced. The similar kinds of allegations surfaced in India too before 2019 elections in the country. The social media, print media, online news, and different news channels can be used as the tools to implement the agenda based on the data achieved from the target audience or a society.

Hence, cybersecurity aspects span a lot of different subjects in today’s world. With the emerging and innovative technologies, we have been benefited as well as new threats and risks have emerged. Meticulous studies could eventually solve issues in the coming days and there is indeed no alternative to continuous research in these domains.

**Sample Questions and Answers**

**Q1. Name some domains where the strongest impact of cybersecurity is noticed due to the emerging technologies**.

**A1**. The strongest impact of cybersecurity due to the emerging technologies is especially noticed in the following domains:

- Risk to National Security
- Breach of Privacy
- Increased Burden of Cybersecurity on Businesses
- Shortage of Cybersecurity Specialists
- Risk of Extensive Data Exposure
- Society & Business Manipulation.

**Q2. What are the reasons for increasing trend of breach of privacy with the emergence of modern technologies?**

**A2**. The breach of privacy keeps increasing with the emergence of the modern technologies due to the following reasons:

- Over excitement of the users to use the newer technologies without knowing or taking care of the impact of those technologies on privacy breaches.
- Early release of products or services based on the innovative technologies by the companies while ignoring the privacy breach issues.
- Unavailability of domain expertise and security professionals to deal with the emerging data breach threats.

**Q3. Why is it difficult to find specialists in cybersecurity when modern emerging technologies are considered?**

**A3**. Most of the users are general users or non-experts. When new and emerging technologies come to the market, most of the people are not aware of the risks involved with them. Even the existing experts need training regarding use of the technology and many cannot simply switch to the new mode of operations. Another factor is that their demand becomes high. Hence, it is often difficult to find specialists in cybersecurity in such situations.

**Q4. Write down the main reasons of data exposures pertaining to modern and innovating technologies.**

**A4**. The main reasons of data exposures pertaining to modern and innovative technologies include the following:

- Use of huge number of devices in highly diverse environments of IoT where a large number of devices run diverse firmware and software.
- Increased number of user accounts with those huge number of devices and related services are also prone to data exposure.
- Mismanagement in password creation, maintenance, and storage by the clients.
- Outdated software and devices that are not updated regular also exaggerate the situation.
- Continual emergence of innovative techniques and ways that people are not fully expert at.

**Q5. Give examples how the society can be influenced by information manipulation over the online platforms**.

**A5**. A good recent example could be the US presidential elections in 2016. In those elections, it is alleged that Russia tried to manipulate the mandate in favor of a particular party by building an opinion in the people in such a way that they would be easily influenced. The similar kinds of allegations surfaced in India too before 2019 elections in the country. The social media, print media, online news, and different news channels can be used as the tools to implement the agenda based on the data achieved from the target audience or a society. For achieving the goal, all types of online platforms can be used.

**Test Questions**

1. How do modern technologies impact cybersecurity?
2. How are the advanced technologies affecting cybersecurity?
3. Extensive data exposure: what are the risks?

4. Is there a strategy for controlling cyber breaches?

5. What is the reason for the shortage of cybersecurity professionals?

6. What impact do cyber-attacks have on businesses?

7. What are the main reasons for data exposure?

8. What is Risk?

9. How can cybersecurity affect national security?

10. What is Zero trust policy?