MMXXII BIMUN

2022 北京国际模拟联合国大会

Beijing International Model United Nations 2022

Background Guide

The Commission on Crime Prevention and Criminal Justice

Topic A: Tackling Cyber-Based Crime through Global Operation

Topic B: Building Resilient Network on Crime Preve-ntion and Governance

Content

Welcome Letter

Dear Delegates,

Welcome to the Commission on Crime Prevention and Criminal Justice (CCPCJ) of Beijing International Model United Nations 2022 (BIMUN2022)! The Directors of CCPCJ would like to extend our warmest welcome to you all.

It is difficult to issue a description of our time. Catalyzed by the ravages of the unabated COVID-19, sweeping chain reactions have taken place on the world stage. The pandemic severely disrupted the functioning of global supply chains, though not yet completely deconstructed, sending cold waves of protectionism and isolationism to the once booming economic globalization. More and more countries have stimulated the pace of policy adjustments with an emphasis on maintaining economic and social resilience and balance. Outstandingly, the relationship between science and technology development as well as productivity has been rewritten by the digital and information era. The ongoing technological revolution is unprecedentedly characterized by a diversified distribution of advantages: the creation of any new technology no longer benefits solely one country or civilization. This has led to the phenomenal acceleration of technological development while urging the international community to deal with commonly accepted norms and standards.

CCPCJ is a tool for building international consensus and promoting the integrity of the domestic justice systems of member states. This time, we have set two topics for the upcoming conference, namely: Tackling Cyber-Based Crime through Global Operation and Building Resilient Network on Crime Prevention and Governance. The first topic aims to reflect on the current barriers to cybercrime governance and to address the realities of the problem. And the second is placed under a broad landscape as we seek to improve the overall resilience of cyber governance and transnational cyber governance.

We strongly encourage delegates to make full use of this Background Guide, which is the result of the joint efforts of the Committee, the academic team, and every staff member of China Foreign Affairs University Model United Nations Association (CFAUMUNA).

A challenging time like this belongs to the youth who have the greatest capacity for learning and creating a more resilient world for the benefit of the world at large. The Directors sincerely wish you all a memorable and fruitful academic journey. We look forward to hearing your voice at BIMUN2022 CCPCJ.

Best Regards,

Commission on Crime Prevention and Criminal Justice

January 2022

Introduction to the Committee

The Commission on Crime Prevention and Criminal Justice (CCPCJ) is the main governing body of the United Nations to guide the activities in the fields of crime prevention and criminal justice, providing resources for technical assistance. It is one of the functional commissions of the Economic and Social Council authorized by the United Nations General Assembly and it collaborates closely with other UN intergovernmental organizations. Through resolutions and decisions, standards and norms, thematic discussions, and expert groups, CCPCJ takes action and promotes policies on crime.

CCPCJ serves as a preparatory organization for the United Nations Crime Congresses. The Commission highlights the implementation of Sustainable Development Goal (SDG) 16, which is about promoting peaceful and inclusive societies and access to fair justice for all in regard to its mandates and priorities extended by the Economic and Social Council (ECOSOC) resolution 1992/22. Upon the request of General Assembly (GA) resolution 46/152, the Commission was established by ECOSOC in 1992 as the principal policymaking body of the United Nations, and it is composed of 40 Member States elected also by ECOSOC.[1&2] In 2006, the United Nations Office on Drugs and Crime (UNODC) expanded the mandates of the CCPCJ, allowing it to serve as a governing body of UNODC and approve the budget of the UN Crime Prevention and Criminal Justice Fund. The UNODC and other interregional and regional institutions around the world make up the UN Crime Prevention

[1] General Assembly resolution 46/152, Creation of an effective United nations crime prevention and criminal justice programme, A/RES/46/152 (18 December 1991), available from https://www.unodc.org/documents/commissions/CCPCJ/GA_Resolution-46-152_E.pdf.

[2] Economic and Social Council resolution 1992/22, Implementation of General Assembly resolution 46/153 concerning operational activities and coordination in the field of crime prevention and criminal justice, E/RES/1992/22 (30 July 1992), available from https://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-22_E.pdf.

and Criminal Justice Programme Network (PNI). [3]

As criminal activities do not end at borders, criminal justice and crime prevention are both extremely challenging and demanding fields to work in. Crime is becoming increasingly transnational with intensified criminal confluence and still limited extraterritorial jurisdiction enforcement. And cyber-based crime is only deteriorating the situation. Therefore, the outcomes of efforts can only be held collectively by the countries and made tangible for the people if we work together and with unanimity. CCPCJ has been, and will keep on intensifying technical cooperation, establishing standards and norms, promoting international cooperation in crime prevention and criminal justice, and in making the fullest use of the knowledge and experience of national and international organizations competent in this field.

[3] United Nations Office on Drugs and Crime (UNODC), "The Commission On Crime Prevention And Criminal Justice," *unodc.org*, Jan. 13, 2022 accessed, https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html.

General Introduction

a) General Idea of the Topic

In the process of digitalization and informatization, there exists a staggering complexity that takes the form of the normalization of epidemics, increasing economic inequality, and the ebbing of globalization. Cyberspace, a borderless realm, casts a giant shadow upon various network malpractices, organized crime groups, and considerable loopholes in legal enforcement. Cyber-based criminal activities therein have also developed. Cyber-based crime takes form both in facilitating the traditional crime and in committing crime through information communication technology (ICT), namely, cyber-enabled and cyber-dependent crime (see "Key Terms" for detailed information.)

In the light of the up-to-date issues and the long-term sustainability of cyberspace, CCPCJ aims to address cybercrime with technical means through initiating two interrelated topics, namely A) Tackling Cyber-Based Crime through Global Operation, and B) Building Resilient Network on Crime Prevention and Governance. Both topics address thorny challenges at various levels of cybercrime governance and, as a result, building a bridge for cooperation among countries to deal with the problem. The scope and aim of both topics are extensively specified by this committee in order to properly examine and meet the issues, as addressed below.

There is a scarcity of technical proficiency while new criminal means are increasing dramatically. The use of traditional methods is stretched to the limit in combating crime in this new space. Topic A focuses on addressing cyber-based, transnational crime under the epidemic context in the drastically changing information age, narrowing the gap between ever-rampaging cyber-based criminal activities and insufficient countermeasures, strengthening the sense and competence of global cooperation in tackling cybercrime, and gathering efforts for a more enabling environment which is safe from cybercriminal practices. The first topic is also set to review the exchanges on administrative and legal branches to improve the quality and efficiency of the response mechanism. It is critical to achieve a comprehensive breakthrough in understanding the upcoming uncertainty in terms of both theoretical and empirical spheres.

The second topic first provides the theoretical elements of cybersecurity, and then draws attention to cyber-based crime penetrating deeply through the network architecture. This is a topic to encourage innovative thinking and sharp observation of cyber community construction. Delegates are expected to first equip themselves with the fundamental knowledge and existing mechanisms of network before taking joint efforts in foreseeing future stages of cyberspace development.

CCPCJ is increasingly concerned about the great challenges posed by the evolving cyberspace and the transnational nature of cybercrime. At the same time, the committee takes note that international organizations also have a greater use for tackling cyber-based crime. This Background Guide is a summary of the committee's complete understanding of the topic. Questions to Consider is an enlightening section helping delegates to understand the issues in depth. And all readers are welcome to put forward their own understanding as well as constructive suggestions. Heated discussion is expected under the topics for youthful and aspiring participants with forward-looking perspectives on cybercrime prevention and criminal justice in the ever-present challenges of the Internet Age.

b) Key Terms

Cyber-Dependent Crime

Cyber-dependent crime is the crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In this type of crime, the computer itself is the target of offence, and negative effects include the damage upon confidentiality, integrity, and availability of computer data or systems. [4]

Cyber-Enabled Crime

Cyber-enabled crime is a form of traditional (offline) crime facilitated by Internet and digital technologies. The ICT plays the role of modus operandi (i.e., method of operation) in this category. Cyber-enabled crime involves the real-space activities and may cause physical damage to the life and property of victims. [5]

Compliance Dilemma

In the context of cybercrime, compliance dilemma is a situation in which the practical need for entities or individuals to assist in cracking down on cybercriminal acts contradicts the regulations or restrictions that the entity or individual was bound to comply with, especially when the perpetrator, law executor, and entity are under the jurisdiction of more than two sovereign states. The overlap of jurisdiction in cyberspace is the main cause of such dilemma, and international coordination is urgently needed to resolve this issue.

[4] UNODC, “Cybercrime in Brief”, *E4J University Module Series: Cybercrime,* Jan. 28, 2022 accessed, https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html.

[5] Ibid.

Topic A: Tackling Cyber-Based Crime through Global Operation

I. Current Situation

a) Overview of the Current Situation

To successfully fulfill its oversight duty, CCPCJ should ensure that the understanding of cyber risk is constantly upgraded, and it must comprehend its role in managing such a threat. The first topic focuses on mitigating the problem where the cybersecurity fundamentals and response mechanisms are too inefficient to cope with the deteriorating cyber-based crime. To better understand the urgency of cyber risk and give suggestions to collaborators as they embrace their position in cybercrime management, we need to have a grasp of the newly-emerged cases, outdated legal instruments, and virtualization of criminal means, as well as the effective countermeasures.

As the product of the Internet age, digital economy, communication tools, and other derivatives are building connections between individuals, reorganizing groups, and reducing the need for face-to-face interactions. While the thrilling technological advancements penetrate almost all aspects of human life, they have also opened up myriad opportunities for perpetrators of cybercrime.[6] With the help of the Internet, illegal instruments are now widely accessible, and criminal activities are more difficult to track, making Internet users more and more likely to become the victims who also find it difficult to speak for their own rights.

On the other hand, cybercrime scholars have struggled to find enough reliable data to perform in-depth study on these new cybercrime cases. At the margins of the 30th UN CCPCJ, a side event titled "Digital is the new normal!" where experts ap-

[6] Bossler, Adam M., and Tamar Berenblum. 2019. "Introduction: New Directions In Cybercrime Research". *Journal Of Crime And Justice* 42 (5): 495-499. doi:10.1080/0735648x.2019.1692426.

pealed for joint efforts to better handle cross-border electronic evidence.[7] Direct access to data from network information providers is expected to be a representative state-of-the-art model.

Worse still, the speed at which cybercrime is updated makes it impossible to follow the relevant legislation and judicial issues in a timely manner, falling into a compliance dilemma. Traditional international mutual legal mechanism of criminal and judicial assistance procedures to address the need for evidence in a timely and effective manner.[8] The solution is stalled by the imprecise definition of new methods, the transnational nature of the resultant judicial incompatibility, and basic variations in law enforcement across countries.

In a shell, cyberspace provides the occasion for new forms of cyberattack, obstacles to coordinated response, and compliance issues. Countries in the Internet age should better foundations to control cyber risks under the rapidly changing cyber-threat landscape.[9] Overall, the written laws, institutionalized protection mechanisms, and feedback loops for combating cybercrime are all immature, which adds to the rising frequency of cybercrime. To arrive at the answers, however, we need to first have a basic grasp of what has been hitherto accomplished.

b) Past Actions

Budapest Convention

The increasingly complex cybercrime landscape urges countries to align their do-

[7] United Nations, “The New Normal Is Digital,” Department of Economic and Social Affairs, Jan. 9, 2022 accessed, https://www.un.org/en/desa/new-normal-digital.

[8] Wei Pei, “Public-Private Cooperation In Cross-Border Combat Against Cybercrime,” *Information Security And Communications Privacy, no. 7 (2021)*: 37-45.

[9] Clinton, Larry, Daniel Dobrygowski, Sean Joyce, and Friso Van der Oord, “*Principles For Board Governance Of Cyber Risk*,” Insight Report, Geneva: World Economic Forum.

mestic cybercrime strategy with international strategies and practices. The Budapest Convention was opened for signature in Budapest, Hungary, in November 2001.[10] As the first convention that addresses crimes committed via the Internet and other computer networks, it mainly focuses on offences against and by means of computer systems and data. The Convention offers the most comprehensive and coherent international agreement on criminalization, procedural law tools, and efficient international cooperation. [11]

The Convention functions through the Cybercrime Convention Committee (T-CY) and Cybercrime Programme Office of the Council of Europe (C-PROC), which forms a consolidated framework to protect people's legitimate interests in using and developing information technologies.

Intended to build the framework for cooperation among Parties to the widest extent possible, the Convention promoted a fast and effective regime of international cooperation, advanced a 24/7 network, and improved interactions with private sectors.[12] The Convention was written to ensure a balance between law enforcement and fundamental human rights while being conscious of the profound changes brought by digitalization, convergence, and continuing globalization of computer networks. [13]

To address today's ever-evolving cybercrime, Parties of the T-CY actively participate in the negotiation of future instruments, and a second Additional Protocol is being developed. Meanwhile, C-PROC complements T-CY's work by encouraging Parties to assist in implementing the Convention. C-PROC continues to offer support in terms of legislation,

[10] Council of Europe, "Actions Against Cybercrime," Council of Europe, Feb. 7, 2022 accessed, https://www.coe.int/en/web/cybercrime/home.

[11] Ibid.

[12] Council of Europe, "Budapest Convention", *Council of Europe*, Nov. 23, 2001, Article 23

[13] Council of Europe, "Budapest Convention", *Council of Europe*, Nov. 23, 2001, Preamble

personnel training, setting up expert groups and promoting cooperation at different levels, and is responsible for the Council's capacity-building efforts. Annual reports have been published by the Office in the context of Covid-19. C-PROC also plans to serve more countries beyond the European border (such as ASEAN countries) and expand its influence globally.

The Global Initiative Against Transnational Organized Crime (GI-TOC)

The Global Initiative Against Transnational Organized Crime (GI-TOC, also short for TGIATOC) was founded in 2013. It was established to provide a forum that involves every part of society and encourages information-sharing and communication worldwide.[14] The 2021-2023 strategy will continue to work towards putting in place the building blocks for a global strategy against organized crime.

Defined as “a network to encounter networks”, the GI-TOC has shown great advantages of reach, inclusiveness, credibility, agility and govenance.[15] These advantages indicate that the GI-TOC offers an efficient and organized platform to relate and assist stakeholders. The three core areas of work include:

i) Providing analysis on organized crime and corruption;

ii) Covering meetings to generate new approaches and stimulate policy debates;

iii) Supporting innovative on-the-ground initiatives.

The initiative has held eight quarterly virtual group discussions since 2019 and

[14] GI-TOC, “Strategy 2021-2023", *Global Initiative Against Transnational Organized Crime*, Jan, 2021

[15] Ibid.

absorbed 143 members worldwide contributing to blogs, podcasts, etc.[16] It has greatly assisted the CCPCJ in enhancing analysis, encouraging action, and supporting resilience in the face of organized crime.

International Criminal Police Organization (INTERPOL)

The International Criminal Police Organization (INTERPOL) aims to enable police around the world to work together to prevent and fight international crime.[17] It offers a unique platform that supports police around the world with targeted training, investigative support, relevant data and secure communication channels.

It is vital that the Police agencies have access to share information and knowledge with their counterparts on the international level to tackle cross-border cybercrime. To boost-co-operation, INTERPOL provides cybercrime collaboration services such as Cybercrime Knowledge Exchange and Cybercrime Collaboration Platform, ensuring a timely, intelligence-based response among police and stakeholders and thereby securing the cyberspace. [18]

The collaboration between CCPCJ and INTERPOL has boosted global alliance against cybercrime and facilitated down-to-earth operations against many types of cybercriminal activities.

Extended Issues

Cybercrime Exacerbated by the COVID-19 Pandemic

The COVID-19 epidemic has added to the uncertainty about the Internet's future.

[16] Ibid.

[17] INTERPOL, "INTERPOL: an overview", *International Criminal Police Organization*, Jan, 2020.

[18] INTERPOL, "Cybercrime Collaboration Services", *International Criminal Police Organization*, Nov, 2020

During the epidemic, the Internet served as both a workplace and a dancefloor for many netizens. The fact was neglected that danger also lurked and was hugely underestimated.

Vulnerability of victims to cybercrime has been aggravated by both the pandemic as well as the fast-growing netizen population. The growing disparity between the rich and the poor as the internet upgrading between traditional and non-traditional industries could not be synchronized. This, in turn, makes the vulnerability of cyberspace even greater and the evidence of cybercrime even more difficult to capture. According to Liu Zhenmin, UN Under-Secretary-General and Head of UN Department of Economic and Social Affairs (DESA) on the 2020 Annual Meeting of the Internet Governance Forum, the post-COVID-19 age will usher in a new normal, one that will hasten digital change across the board. Digital economy, digital finance, digital governance, digital health, and digital education are examples of these. Many governments and corporations, in fact, have already embraced digital platforms and solutions. The COVID-19 epidemic, on the other hand, has highlighted severe vulnerabilities and digital inequalities that have been allowed to grow for far too long. [19] At the same time, dangerous falsehoods can now travel quicker and wider because of the Internet. While it has the potential to be a true weapon of human resilience and unity, it could take a long way to bring that vision to reality.

Anriette Esterhuysen, Chair of the Forum's Multistakeholder Advisory Group, also pointed out that information sharing platforms are necessarily representing the extraordinary role that the Internet has been playing during COVID-19 pandemic, and will take a people-centered approach to network resilience, looking at how it has aided human resilience and solidarity in the face of the pandemic's various obstacles. [20]

II. Problems to be Solved

[19] United Nations, "The New Normal Is Digital," Department of Economic and Social Affairs, Jan. 9, 2022 accessed, https://www.un.org/en/desa/new-normal-digital.

[20] Ibid.

Technically speaking, the core issue to be tackled under this topic is not cybercrime itself, but the aggravation and intensification effect of the Internet on criminal activities. The advent of networks, information and communications technology (ICT), and cyberspace has brought an enormous transformation to all aspects of traditional crime, including the criminal, victim, space of crime, modus operandi (method of operation), and the damage caused. In brief, the Internet has exacerbated the problem of cybercrime by facilitating its rapid evolution, expanding the scope of its impact, masking the criminals, increasing the vulnerability of potential victims, concealing the evidence, virtualizing the criminal means, deconstructing and blurring the concept of criminals and victims, and creating barriers against legal investigations and criminal justice.

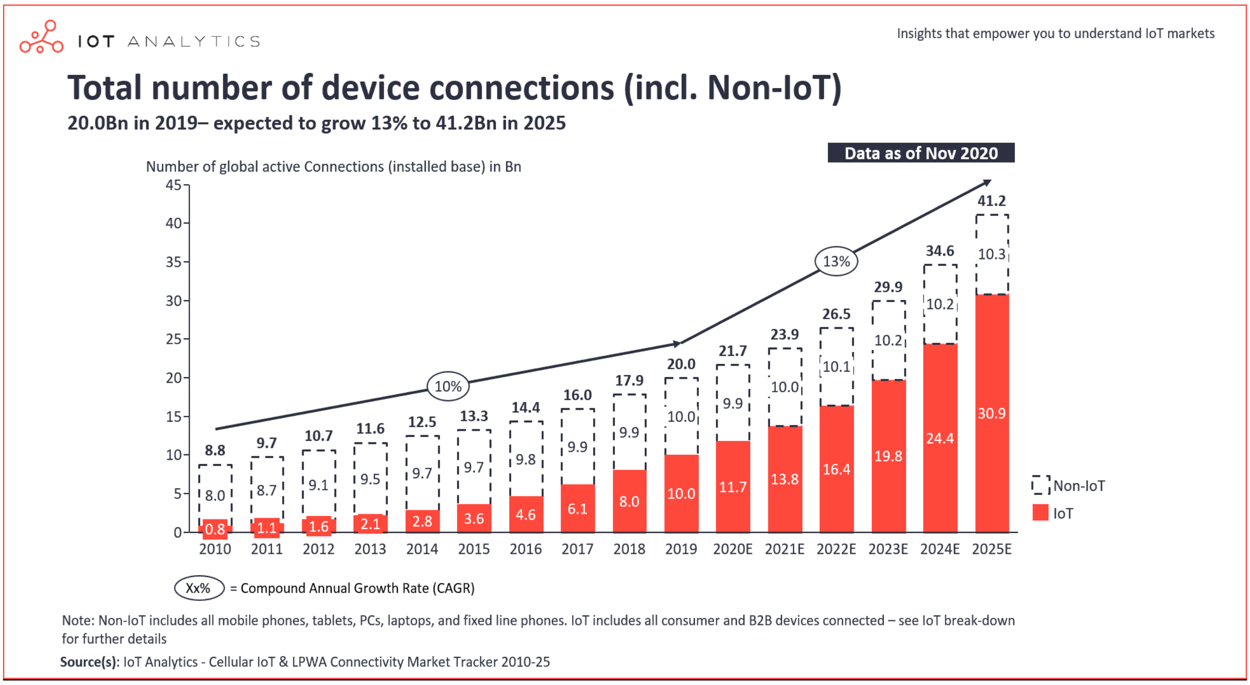
a) The Rise of Newly-Emerged Cyber Offenses

i. Fast-Evolving Cybercriminal Means and Channels

With the digital transformation in full swing, the world is taking one step further into cyberspace. The information and communication technology has not just enabled a higher-quality socioeconomic development, but also facilitated the growth of many cybercriminal activities. For example, the now-commonplace use of online payments has given rise to consumer financial fraud. Global incitement to violence and terrorism through social media has widened the reach and influence of previously localized radical and terrorist groups. Purchasing of many illicit products such as drugs and weapons can be done more insidiously on the internet. The anonymity of the Internet and the possibility of adopting flexible identities can be incentives for even more criminal behavior. [21]

[21] CCPCJ, "New and Emerging Forms of Crime: Threats the World Must Reckon With," *13th United Nations Congress on Crime Prevention and Criminal Justice,* Apr. 2015, Feb. 11, 2022 accessed, https://www.un.org/en/events/crimecongress2015/pdf/Factsheet_5_Emerging_forms_of_crime_EN.pdf.

Another remarkable trend is the increase of online services. Daily services such as dining, shopping, social networking, travel booking, payment, and entertainment are rapidly integrated with information technology, along with the advent of multitudinous apps and online platforms. Each newly-emerged channel, however, brings yet another risk for potential attack and technology abuse to happen.



Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

Figure 1 Total Number of Device Connections Worldwide by 2025

The Internet of Things (IoT) contributed to a scaleup of cyberattack surface. The IoT market analysis anticipated a 30+ billion IoT connections worldwide by 2025 (as is shown in the Figure), and approximately 4 IoT devices per person on average.[22] The innovation of digital tools and increase of access to Internet provided more approaches than ever for offenders to operate. Data is the building block of the digitized economy, and the exponential growth of data storage is projected to exceed 200 zettabytes by 2025.[23] A larger storage means greater burden of data

[22] Knud Lasse Lueth, "State of the IoT 2020: 12 Billion IoT Connections, Surpassing Non-IoT for the First Time", *IoT Analytics*, Nov. 19, 2020, Jan. 11, 2022 accessed, https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

[23] Steve Morgan, "The World Will Store 200 Zettabytes of Data by 2025", Cybercrime Magazine,

protection, as well as increased risk of information misuse and privacy abuse. In this context, hackers are granted ever more options to breach cyber-defense and exfiltrate data. [24]

ii. Increasingly Vulnerable Internet Users

Today's society has seen a massive "immigration" of netizens into the virtual world. The global Internet penetration rate has risen from 16.8% in 2005 to 51.4% in 2019, and in 2020 there are estimated to be over 2525 million Internet users in Asia alone.[25] The expansion of online population comes along with a wider variety of age groups engaged in online activities, in particular, the children and the elderly. Statistics show that in 2021, 73% of Americans over the age of 65 use the Internet, compared to 14% in 2000;[26] and 60% of American children are engaged with smartphones (the percentage being 44% in the case of desktop or laptop computer) by the year 2020. [27] These internet users are comparatively lacking of sound judgement and anti-fraud capabilities, and therefore are more likely to fall victim to various cyber offences.

Jun.8, 2020, Jan. 15, 2022 accessed, https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/.

[24] Chuck Brooks, "3 Key Cybersecurity Trends to Know for 2021 (and On...)", Forbes, Apr. 12, 2021, Jan. 11, 2021 accessed, https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/?sh=77782cc49786.

[25] Joseph Johnson, "Global Internet Access Rate 2005-2019", Statista, Jan. 27, 2021, Jan. 12, 2022 accessed, https://www.statista.com/statistics/209096/share-of-Internet-users-in-the-total-world-population-since-2006/.

[26] Nikola Djordjevic, "The Elderly and the World Wide Web", MedAlertHelp.org, Jan.5, 2022, Feb. 10, 2022 accessed, https://medalerthelp.org/blog/elderly-the-world-wide-web-infographic/#:~:text=And%2C%20when%20it%20comes%20to%20the%20Internet%2C%20age,Internet%20usage%20to%20three%20or%20five%20times%20weekly.

[27] Brook Auxier, "Children's Engagement with Certain Types of Digital Devices Varies Widely by Age", *Pew Research Center,* Jul. 28, 2020, Feb. 10, 2022 accessed, https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/.

As remote working or home-officing gains popularity in the recent decade, more Personal Computers (PCs) are becoming engaged in online businesses. Nevertheless, home offices are much less protected than the fortified office sites, which are often secured by firewalls, routers, and access management run by the company. Remote employees and their devices have thus become an easy target of cybercriminal offences.

Social media and networking platforms have begun to reign supreme in people's everyday entertainment. Netizens are motivated to post, receive, and repost messages, photos, or videos containing personal information that may well be utilized as a threat to their own security. Furthermore, the platforms themselves may serve as channels of communication for illicit activities both online and offline. These factors all added to the vulnerability of the mass online population.

iii. Expanded Range of Potential Damage

Cyber-dependent crimes are a mere tip of the iceberg, as more serious damages begin to spill over from the virtual world into the real one. As the Internet further integrates with people's daily life, cyber-enabled crimes began to pervade. In 2020, the Nth Room Case in South Korea shocked the world by revealing how perpetrators were able to implement real-life sexual exploitation and abuse of over 100 victims with some simple taps on the phone. Pay-to-view chat rooms were established and operated on a chat app Telegram, where managers distributed videos of school girls (including the underage) performing grotesque sexual acts and self-harm. [28] Between the online offenders and offline victims are the intermediate links of blackmailing, privacy abuse, and intimidation. Apart from online child sexual exploitation and abuse, cyber-enabled interpersonal offenses further include cyber-harassment, cyberbullying (the type of cyber-harassment featuring the involvement of minors), cyberstalking (the type of cyber-harassment featuring direct or

[28] Nicole de Souza, "The Nth Room Case and Modern Slavery in the Digital Space", *The Interpreter*, Apr. 20, 2020, Jan. 13, 2022 accessed, https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space.

implied physical harm to the victim), online intellectual property crime, and others. Digital transformation has enabled cybercrime to break the limit of online platforms and penetrate into people's physical lives, directly threatening the life, health, property, and other aspects of citizens.

b) Obstacles to Efficient Joint Response to Cybercrime

The newly-emerged cyber offenses posed serious challenge to the law enforcement in cyberspace. The anonymity and indirectness of cyber-activities provide disguise for behind-the-screen criminal attempts, and the difficulty in confirming criminal identities further hinders the progress of investigation.

i. Inadequate Control Instruments for Law Enforcement

The Internet was initially designed for military or academic purposes, under the assumption of a benign and trustworthy user community. By and large, the design parameters of the Internet are far exceeded by the threat environment in recent decades. The network involves a decentralized design which seeks to keep its main functionality intact even when components of the network were attacked. Nonetheless, the decentralized architecture led to a degree of inadequacy in facilitating criminal investigations or preventing attacks from within the network. [29]

There are some existing cybersecurity measures in response to the rise of cyber-dependent crime, such as user authentication (usually with passwords, PINs, or biometrics) and access control [30]. However, less control instruments are in place for the investigation and

[29] CCPCJ, "Report of the Open-Ended Intergovernmental Expert Group on the Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector", *ECOSOC*, Apr. 11-15, 2011, Jan. 13, 2022 accessed, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V11/803/26/PDF/V1180326.pdf?OpenElement.

[30] UNODC, "Cybersecurity Measures and Usability", *E4J University Module Series: Cybercrime*, Apr. 2019, Jan. 13, 2022 accessed, https://www.unodc.org/e4j/en/cybercrime/module-9/key-is-

law enforcement of real-life offenses facilitated by ICT technology.

ii. Difficulty in Tracking Offenders

Tracking offenders involves both online and offline operations. The Internet Protocol (IP) addresses that used to link users to a specific range are no longer trustworthy, since they are easy to tamper with and create false source addresses that can be misguiding [31]. Furthermore, unlike telephone services which entails tracking and billing on a per-call basis (in order to charge users of its service), Internet services seldom require service providers to track the fine-grained behavior of customers, but rather base their charges on large-grained service provisions such as monthly connectivity, connection speed, and storage capacity [32]. Multiple anonymizers that are used to protect user privacy also impedes criminal investigation online. Moreover, netizens' demand for high-speed (or high-bandwidth) Internet outweighed the investigators' demand for evidence saving. The routers are designed to push the packets through as quickly as possible instead of processing the data, therefore is unable to highlight any suspicious data or store it for a long enough period of time.

Offline tracking is even more complicated, because cybercriminal activities are often cross multiple administrative, jurisdictional, and national boundaries. For lack of universal standards for monitoring, record keeping, and information sharing essential to tracking criminals, investigation efforts are often met with barriers.

iii. Volatility of Digital Evidence

Digital evidence is defined as "information and data of value to an investigation that is

sues/cybersecurity-measures-and-usability.html.

[31] Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy", *Carnegie Mellon Software Engineering Institute*, Nov. 2002, Jan. 14, 2022 accessed, https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf.

[32] Ibid.

stored on, received, or transmitted by an electronic device"[33]. This type of evidence is vital in the forensics for cyber-enabled crimes. Unlike physical evidence such as objects and fingerprints, digital evidence is intangible, and can be easily altered, damaged, or destroyed. Even after acquiring the evidence, improper handling may still disturb the information it contains. The volatility and fragility of digital evidence require careful handling and coordination between first responders (persons among the first to arrive at the crime scene) and investigators, especially in case of cross-administrative cybercrime. The time-sensitive feature of digital evidence demands timely response and highly-efficient transnational operation. At the current stage, cross-administrative coordination in digital forensics remains insufficient.

c) Compliance Dilemma

Compliance dilemma [34] can be caused by different factors, including the gap in criminalization of certain cyber-based activities, the conflict between territorial jurisdiction and extraterritorial jurisdiction, and more often than not, a number of weak links within a chain of cybercriminal law enforcement.

It is to be noted that, the compliance dilemma is the result of both imperfections of the traditional legal framework and insufficient mechanism building for global operation. The mandate of CCPCJ, however, focuses on optimizing the global operation mechanisms in order to complement the legal deficiencies, instead of the other way around.

i. Inconsistent Pace of Criminalization

[33] David W. Hagy, "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition", *U.S. National Institute of Justice*, 2001, Jan. 15, 2022 accessed, https://www.ojp.gov/pdffiles1/nij/219941.pdf.

[34] Pei Wei, "On the Enforcement Jurisdiction in Cross-Border Data Investigation against Cybercrime", *Journal of Comparative Law,* Nov. 23, 2021, Jan. 15, 2022 accessed, https://kns.cnki.net/kcms/detail/11.3171.d.20211122.1425.002.html.

Criminalization of cyber offenses are the precondition for criminal justice and law enforcement. This is especially the case in transnational cybercrime, in which dual criminality plays a critical role. Dual criminality is a principle which stipulates that the alleged crime for which extradition is being sought must be criminal in both the demanding and the requested countries. [35]However, the law and regulations may vary significantly among different jurisdictions, creating barriers for law enforcement agencies in one country to track down cybercriminals located overseas. For example, although many multilateral law instruments have criminalized illegal access to computer systems, illegal interception, illegal computer data and system interference, and the misuse of devices, other areas have received relatively little attention in international treaties. These areas include:

i) Violation of data protection measures for personal information;

ii) Breach of confidentiality;

iii) Use of forged or fraudulently obtained data;

iv) Illicit use of electronic payment tools;

v) Acts against privacy;

vi) Disclosure of details of an investigation;

vii) Failure to permit assistance. [36]

Another area of concern is the newly-emerged cyber-enabled offenses, which keeps

[35] Britannica, “Double Criminality”, *Britannica*, Jan. 14, 2022 accessed, https://www.britannica.com/topic/double-criminality.

[36] Emilio C. Viano, “Cybercrime: Definition, Typology, and Criminalization”, *Springer International Publishing*, Dec. 13, 2016, Jan. 15, 2022 accessed, https://doi.org/10.1007/978-3-319-44501-4_1.

evolving into diverse criminal approaches that exceed the boundary of current criminalization. The different criminality standard between jurisdictions and lacking of harmonization caused inconveniences in law enforcement. To make matters worse, due to the prominent criminalization gap (namely criminals might conduct cyber offenses in a country where it is considered legal, while causing damage upon another country where such offenses are criminalized), many attackers or offenders are incentivized to gather in countries with more relaxed laws on cybercrime, turning some underdeveloped countries into cybercriminal hideouts and exacerbating the cybercrime issue globally.

ii. Conflict of Jurisdiction

Cybercrime may transcend the traditional notions of physical borders and challenge the jurisdiction of sovereign states. In cyberspace, the boundary between different jurisdictions is often blurred by the free transborder flow of data. The complexity of cyberspace boundaries can be exemplified by the France v. Yahoo! case in 2006, in which the US-based web service provider Yahoo! was sued for its sale of Nazi memorabilia to French citizens on the company's website. Arguments raised by the Yahoo! include its right to freedom of speech (under the protection of US laws), the infeasibility of exclusively blocking an internationally-available website from the French people, as well as the fact that removing Nazi memorabilia will lead to a passive global compliance to French domestic laws.

The case was closed upon discovering that Yahoo! was in effect able to identify and block no less than 90% of netizens located in France (using a newly-developed IP identification technology), and Yahoo! was ruled by court to block its sales in France to the best of its ability [37]. The ban on sales of Nazi memorabilia in France raised questions about whose laws apply to websites that can be viewed worldwide, as well as whether courts in one country should be able to assume jurisdiction over the activities of service providers

[37] Wu Qi, "Jurisdiction Conflicts and Resolutions in Cyberspace", *Journal of Southwest University of Political Science & Law*, vol. 23, no.1: 48-49.

overseas. This case also revealed that advanced technologies may contribute to solving the jurisdiction puzzle in cyberspace .[38]

iii. Transregional Capability Gap in Law Enforcement

The Cannikin Law (or the Wooden Bucket Theory) suggests that a bucket's capacity is determined by its shortest stave. The same is true with the capacity for cybercriminal law enforcement across the globe. International cybersecurity is a chain in which the failure of any weak link may easily offset the global effort to combat cybercrime.

The deficit in national capacity mainly results from inadequate personnel, finance, and technical resources. First, the quantity and quality of personnel needed to investigate cybercrime, prosecute cybercriminals, and handle international cooperation requests may be insufficient in some countries. Second, financing is crucial in recruiting, hiring, and keeping qualified personnel, as well as supporting regular and up-to-date training initiatives. Third, many countries lack the facilities to analyze digital evidence, and funds for purchasing digital forensics tools. [39] And finally, innovation is inevitable in face of the newly-emerged cybercriminal means, while many developing and underdeveloped countries fail to master the core technologies in this respect. International cooperation and partnerships are urgently in need to complement the digital gap between developed and developing nations, and global operation mechanisms need to be established for countries to better join hands in the fight against cybercrime.

III. Possible Solutions

[38] Richard Waters, Patti Waldmeir, “Yahoo Loses Nazi Memorabilia Case", *Financial Times,* Jan. 13, 2006, Jan. 15, 2022 accessed, https://www.ft.com/content/81127f12-83cb-11da-9017-0000779e2340.

[39] UNODC, “National Capacity and International Cooperation", U*nited Nations Office on Drugs and Crime*, Jun. 2019, Jan. 15, 2022 accessed, https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/national-capacity-and-international-cooperation.html.

a) Optimizing Existing Legal and Technical Instruments

i. Constant Update of Cybercriminal Trends

It became noteworthy in recent years that cyber-enabled crime (which leads to a higher rate of offline damage) has begun to prevail, and the cyber-offenders have been transforming from high-skilled hackers to ordinary netizens. In this context, it is important for law enforcement and criminal justice departments to keep in step with the latest development trends of cybercriminal offences, getting acquainted with their tools, approaches, channels/platforms, technique, etc. The Open-Ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study on Cybercrime has put forward plans to improve database-building and ensuring regular updates of information on new cybercriminal trends [40]. A constant update of these information may help promote the criminalization of new-form offenses, and the development of countermeasures internationally. To ensure the quality, accuracy, and timeliness of these updates, greater efforts should be put into internet surveillance, monitoring, and information exchange on a global scale.

ii. Compiling Inventories of Cases and Best Practices

Unlike laws regarding crime in real space where cases are often precedented and have a wide range of codes and practices for reference, cybercriminal laws are relatively raw and unreferenced. Apart from transforming real-space laws and applying them to cyberspace, it is of equal importance to compile inventories and sources of reference for criminal justice in cyberspace. In 2015, the CCPCJ launched the cybercrime repository, a central database of legislation, case law and lessons-learned on cybercrime and electronic evidence, which aims to assist countries in their efforts to better prevent and prosecute cybercrimi-

[40] UNODC, “Report on the Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime Held in Vienna from 27 to 29 July 2020", *United Nations Office on Drugs and Crime*, Aug. 24, 2020, accessed Jan. 18, 2022, https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/UNODC_CCPCJ_EG.4_2020_2/UNODC_CCPCJ_EG.4_2020_2_E.pdf.

nals. [41] The accumulation of cases and practices may offer clues for handling subsequent cases of similar characteristics, and can be applied in the training of skilled investigation personnel.

iii. Promoting Flexible and Anticipatory Mutual Legal Assistance (MLA)

Mutual Legal Assistance (MLA) often refers to bilateral treaties/agreements in which two states agree to provide, upon request of the other state, the widest measure of legal assistance for investigation, prosecution, and judicial proceedings in relation to a certain crime. Though the operations are usually bilateral, the agreement can be adopted in multilateral frameworks such as international conventions and treaties. Currently, the common MLA frameworks in practice are mainly applied to crimes in real-space, and are yet to be adapted to cyber-enabled offenses and handling digital evidences. Furthermore, many MLAs take the form of inventories that list the specific criminal acts to which the MLA shall apply, while the newly-emerged cybercriminal offences are often left off the list. It is not always practical to update the MLAs synchronously, since it takes a considerable amount of time for any criminal act to emerge, become noticeable, be legally criminalized, and finally be included in the MLA treaties. Therefore, one alternative is to transform the fixed lists into something more extensible and anticipatory, such as descriptive clauses which leaves the door open for crimes of similar feature that may potentially appear in the future.

b) Removing Barriers against Swift Response to Cybercriminal Emergencies

Some cases of cybercrime entail threats that may, if not handled in time, trigger crises that lead to severe loss of life and property. There are also circumstanc-

[41] UNODC, “Cybercrime Repository”, *United Nations Office on Drugs and Crime*, Jan. 19, 2022 accessed, https://www.unodc.org/unodc/es/cybercrime/cybercrime-repository.html.

es where the victim is still being assaulted at the very moment of investigation. In these cases, swift response is key to minimizing losses and preventing further damages.

i. Stabilizing Digital Forensics and Transborder Access to Electronic Evidence

Digital forensics is concerned with recovering the volatile information that may have evidential value. The integrity and authenticity of electronic evidence have a direct bearing on the weight of evidence, in terms of its reliability and trustworthiness. In court trials, the party seeking to introduce evidence are often required to demonstrate the continuity, or "chain-of-custody" of the evidence to prove that the evidence has not been tampered with or otherwise altered[42] . Smooth handover is required in order to maintain a sound and complete chain of custody during the cross-border transmission of electronic evidence. Furthermore, down to earth cooperation should be established not just between governments, but also between investigation departments and private sectors who own the crucial information. More efforts are to be made in ensuring the compliance of all entities in the process of forensics, and sustaining the supply of the evidences during trial.

Access to extra-territorial evidence from clouds and service providers is another issue to be tackled, since barriers often occur due to internet companies' user privacy agreements that aim to protect the information generated via the services they provide. Governments are equally unwilling to share valuable data for fear of data breach or disclosure of confidential messages. In this case, the whitelist for mutually accessible data should be appropriately expanded, and a balance shall be found between protecting national cybersecurity and cooperating against cybercrime.

ii. Building Effectual Joint Investigation Mechanisms

Cybercrime is typically global in nature, with malicious cyber actors operating all over the

[42] UNODC, "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*, (Feb. 2013): 157-159.

world and transcending geographical boundaries. [43] Therefore, appropriate coordination between countries in law enforcement is vital in combating transregional cybercrime. Nowadays many countries have successfully conducted joint investigations of cybercrime, but only few of their outcomes were consolidated into applicable mechanisms. In 2021, the Council of Europe and the European Union Agency for Criminal Justice Cooperation (Eurojust) conducted a workshop that discussed issues regarding joint investigation on cybercrime. The workshop sought to stimulate the coordination of investigations and prosecutions between the competent authorities in EU member states by facilitating the execution of international MLAs, the implementation of extradition requests, as well as the establishment of Joint Investigation Teams (JITs) .[44]

Mechanism-building in joint operations may well contribute to closing the capacity gap between countries, and preventing cybercriminals from abusing the capacity loopholes. Moreover, when an investigation team composes of personnel from both (or all) parties concerned, it becomes easier to overcome the compliance dilemma by properly negotiating over discrepant restrictions and regulations.

iii. Improving Operability of Emergency Response

Even when the compliance dilemma is solved and international coordination is achieved, problems still remain in terms of the cybercrime incident response. The operability of emergency operation is insufficient for want of common standards and emergency response plans and practices. There are multiple measures to enhance the operability. For instance, many countries have set up 24/7 contact points (namely ones that operate 24

[43] Nyman Gibson Miralis, “International Cross-border Cybercrime Investigations: Recent Developments”, *Lexology.com*, Jan. 10, 2019, Feb. 11, 2022 accessed, https://www.lexology.com/library/detail.aspx?g=29aa9398-dd82-49b1-b48f-43586dc6e0e6.

[44] Council of Europe, “Council of Europe and Eurojust Joint Workshop on International Cooperation in Cybercrime: Joint Investigation Teams/Joint Investigations”, *Council of Europe Portal,* Oct. 2021, Jan. 21, 2022 accessed, https://www.coe.int/en/web/cybercrime/council-of-europe-and-eurojust-2021-annual-meeting-jits# {%22107800064%22:[0]}.

hours per day and 7 days per week) to provide immediate assistance in case of emergency.[45] Moreover, the development of specialized investigative powers improves the efficiency of investigations by enhancing the proficiency of personnel. [46]

c) Multilateral and Multisectoral Coordination

i. Harmonizing National Jurisdiction for Transborder Cybercrime

Effective law enforcement is crucial to an open and reliable cyberspace. And the enforcement of substantive law is guaranteed by national jurisdiction. Likewise, through national jurisdiction, the implicit justice of procedural laws is served. Therefore, harmonizing national jurisdiction is the cornerstone of securing a safe, clean and connected cyberspace.

There are two types of international cooperation on transborder cybercrime. The formal mechanisms include bilateral and multilateral cybercrime treaties in which provisions, both procedural ones and substantial ones, are stressed. Other mechanisms that facilitate international cooperation in investigating and prosecuting cybercriminals are mutual legal assistance and extradition treaties. [47] These treaties feature a rather limited scope of cooperation, with a prompt response required.

The two main factors in requirements for international cooperation are dual criminalization and international human rights and obligations. Unlike the latter, which offers a guideline in principle, dual criminality is a substantiative and practicable standard that

[45] UNODC, "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime,* Feb. 2013, P212.

[46] UNODC, "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime,* Feb. 2013, P125.

[47] University Module Series Cybercrime, "Module 7 International Cooperation Against Cybercrime", UNODC, Feb. 11, 2022 accessed, https://www.unodc.org/e4j/en/cybercrime/module-7/index.html.

protects the interest of both the requesting and requested Party.

ii. Enhancing Roles of Service Providers and Private Sectors

The prevention and investigation of cybercrime depend on numerous different elements. The Internet industry is built up by private sectors, and service providers are a crucial part of private sectors. Due to the Internet structure, even the seemingly simplest actions via the Internet involve several service providers, requiring coordination of devices on different layers as demonstrated in the OSI model, a standard system for interconnecting computers or communication systems. To better promote the investigations of cybercrime, the role of these service providers should not be neglected.

One major challenge concerning service providers in law enforcement is measuring how much responsibility they should bear, especially in cases where the service they provided are utilized as either a tool or a channel of cybercriminal activities. Besides, they are often unable to prevent the crime in the first place, thus imposing undue liability on service providers may impact their cooperation on cybercrime investigation. In the face of this situation, some countries involve the Internet industry in criminal investigations on a voluntary basis; other countries impose legal obligations on it. Either way, the roles of private sectors need to be enhanced and advanced.

Measures need to be taken to consolidate cooperation between the private sector and law enforcement agencies. For one thing, private sectors' roles need to be mapped out under the fundamental principle of differentiated responsibilities. For another, practices of the prevention and investigation of cybercrime within the private sector need to be carried out. At the same time, public sectors may establish diversified mechanisms to promote co-operation, including incentivizing, macroeconomic regulations, administrative punishments and so on. All stakeholders need to be rallied up to tackle cybercrime.

iii. Reciprocal Green-Channel Agreements

It is commonly held that there are two dimensions of national sovereignty, internal and external. With the external sovereignty featuring interdependence, an efficient and symmetric set of international agreements is needed to strike a balance between crime-solving and protection of state sovereignty.

These agreements are mainly targeted at cyber-enabled crimes that involve more than one country. Mutual assistance and prompt response are required. In such cases, not only the legitimate rights and sovereignty of the requested Party but also the urgency and significance of cooperation need to be considered. For example, in a domestic cybercrime case whose sole requirement for international support is obtaining evidence abroad, reciprocal Green-Channel agreements would facilitate a time-efficient response concerning rights and requests from both Parties. [48]

For serious cybercrime offences repeatedly occurring around the world, building bilateral or multilateral green channels would greatly raise the efficiency of law enforcement and national jurisdiction. Supported by current legitimate protocols and agreements, such channels encourage domestic stakeholders to assist overseas cybercrime investigation. At the same time, mutual assistance for domestic cybercrime is ensured.

Topic B: Building Resilient Network on Crime Prevention and Governance

I. Current Situation

a) Overview of the Topic

Topic A presents us with a number of empirical cybercrime challenges, while Topic B encourages us to foresee future stages of cyberspace development within the

[48] Wei Pei, “Law Enforcement Jurisdiction in Cross-border Data Forensics of Cybercrime”, Study of Comparative law, no.6 (2021).

network architecture. During the discussion under this topic, we present the theoretical models of the cybersecurity framework before dealing with the network resilience-building on crime prevention and governance. The significance of this topic stems from our awareness of the quick changes in today's online world on the one hand, and, on the other, our investigation into the feasibility of creating a vigorous, long-lasting cyberspace.

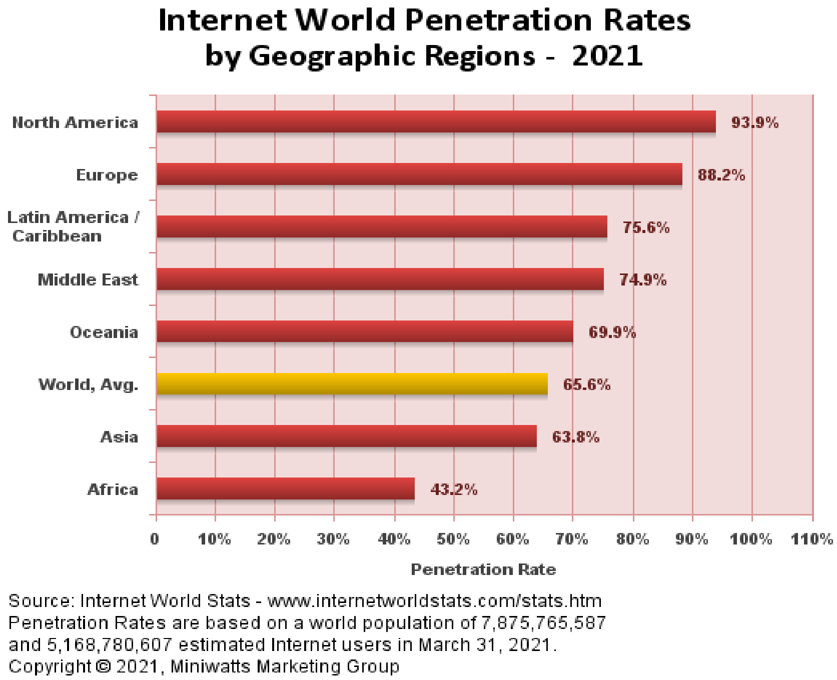
The spread of cyberspace has expanded at an alarming rate as a result of the impact of informatization on communication technologies, inexorably driving the process of globalization and privatization while combating the trend of counter-globalization. And such interaction is responsible for the intensified digital and information technology divide. Various countries with diverse and varied experiences have developed strategies to bridge this gap. [49]

At the same time, cyberspace's hazy and erratic boundaries allow it to penetrate deeper and more invisibly into the economic, social, and political arenas. States, corporations, and individuals are increasingly realizing that cyberspace challenges are intricately related to other domains and that they must respond quickly. [50]

The Internet is not only expanding outward, but also penetrating inward. On the flip side, the number of Internet users is growing. The figures for 2021 suggest that global average Internet usage is fairly high, as illustrated in Figure 1, and the upward trend shows no indications of abating. The demand for cyberspace stability and uniformity has risen from the national level to include an increasing number of Internet users.

[49] Rogers, M. Everett. 2015. "The Internet And Sustainable Development". *UNESCO-Encyclopedia Of Life Support Systems (EOLSS) II*. Accessed Jan. 10, 2022. https://www.eolss.net/ebooklib/sc_cart.aspx?File=E6-33-03-05.

[50] Daniel Goldstein, Hogan-Burney, and Manky. 2020. “Partnership against Cybercrime.” *Insight Report*. Geneva: World Economic Forum. Accessed Jan. 17, 2022. https://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf.



Internet World Penetration Rates
by Geographic Regions - 2021

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,875,765,587
and 5,168,780,607 estimated Internet users in March 31, 2021.
Copyright © 2021, Miniwatts Marketing Group

Figure 1 Internet World Penetration Rates by Geographic Regions - 2021[51]

Under this topic, we aim to stimulate creative thought and keen observation of cyber community development. After preparing themselves with essential knowledge of the cybersecurity framework, delegates are encouraged to touch upon enhancing the holistic data protection mechanism, upgrading the network governance paradigm, and securing the use of personal information.

b) Explanation on Cybersecurity Framework

Before we touch upon the arousing problems and their pertinent solutions concerning cyber security, we should get hold of the fundamental elements that constitute the internet on which cyberspace and cyber security measures heavily de-

[51] Penetration Rates are based on a world population of 7,875,765, 587 and 5,168,780,607 estimated Internet Users in March 31, 2021. Miniwatts Marketing Group, 2021. “Internet World Penetration Rates by Geographic Regions – 2021.” *Internet World Stats.* Accessed Jan. 16, 2022, https://www.internetworldstats.com/stats.htm.

pend.

Generally speaking, the Open System Interconnection Reference Model, more familiarly known as the OSI model, is the accepted standard that explains the computer network architecture with a hierarchical taxonomy. According to this theory, the network structure can be seen as a seven-level vertical architecture. As the level rises higher, the process on the level goes further into the virtual world.

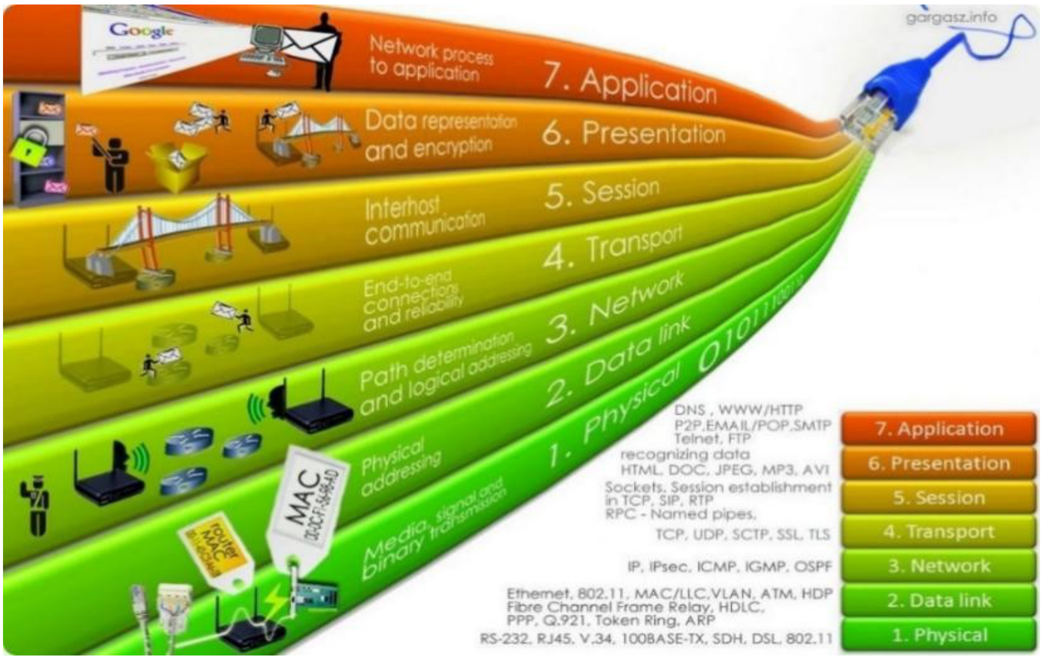

gargasz.info
Google
Network process to application
7. Application
Data representation and encryption
6. Presentation
Interhost communication
5. Session
End-to-end connections and reliability
4. Transport
Path determination and logical addressing
3. Network
Physical addressing
2. Data link
Media, signal and binary transmission
1. Physical 01011100
MAC
router MAC
DNS , WWW/HTTP
P2P,EMAIL/POP,SMTP
Telnet, FTP
recognizing data
HTML, DOC, JPEG, MP3, AVI
Sockets, Session establishment
in TCP, SIP, RTP
RPC - Named pipes.
TCP, UDP, SCTP, SSL, TLS
IP, IPsec, ICMP, IGMP, OSPF
Ethernet, 802.11, MAC/LLC,VLAN, ATM, HDP
Fibre Channel Frame Relay, HDLC,
PPP, Q.921, Token Ring, ARP
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical

Figure 1 The Illustration about the OSI Model [52]

From the bottom of the hierarchy to the top, as illustrated in Figure 1, there are physical level, data-link level, network level, transport level, session level, presentation level and application level. Each level opens up for interactions between certain subjects through respective forms of mediums.

The physical layer props up network communication by the physical properties of the network, which are to send the interpreted physical signals to the other end like fiber-optic cables.

[52] "The OSI model and the TCP/IP stack detailed description", Patches, Accessed January 13, 2022, https://oracle-patches.com/en/cloud-net/the-osi-model-and-the-tcp-ip-stack.

The data-link layer communication is enabled by data-links for Media Access Control (MAC) addressing that further put the network user in connection with the Ethernet, the ubiquitous branch form of the Local Area Network (LAN) after the Address Resolution Protocol (ARP) protocol converts the Internet Protocol (IP) address to its corresponding MAC address from the physical layer.

The network layer is enabled by routers that send information through packets from one logical network to another. Routers can understand the IP address and route the information to the receiver side.

As we keep climbing up to the transport layer, this level ensures reliable end-to-end message transmissions where the Transport Control Protocol (TCP) and the User Datagram Protocol (UDP) come into force to prevent data loss in the host-to-host communications. Whether the message is in the form of a file or streaming video, the two protocols will maintain orderliness throughout the information transmission process.

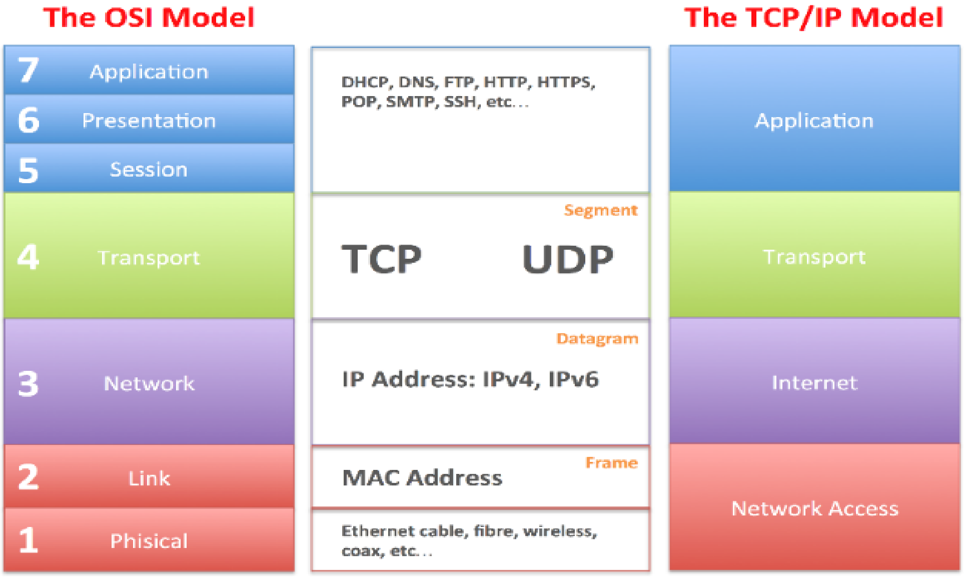
Since every data transmission has been done on the transport layer, the following session layer works to manage the connection between the two end-point users. On this layer, the users finally start to communicate back and forth based on the transmitted information supported by the lower layers and make the interaction a conversation. [53]

The presentation layer goes deeper in the communication process and zooms in for the information format. Up till now, the communication is still filled with messages in binary codes, which are understandable to the devices but utmost confusing to the network users. Represented by ASCII and Unicode, binary interpretations translate the binary language to accessible messages that the message recipient can apprehend.

[53] Glenn Surman, "Understanding Security Using the OSI Model," Sans Whitepaper, accessed January 15, 2022, https://www.sans.org/white-papers/377/.

At the crest of the network architecture, we have the application layer that comes down from information to the users ourselves. All the users' operations can be considered the application interaction between the users and the enormous IT resources, like sending WeChat messages or reading files.

The traditional OSI model illustrates the underlying logical process of the modern age information transfer. Compared to a logical taxonomy, the TCP/IP model systemizes the process from the diametrically opposite end of logical reasons and becomes more commonly used to categorize cybercrimes. This model displays more of a function-oriented picture of IT interactions, as illustrated in Figure 2:



This image is part of the Bioinformatics Web Development tutorial at http://www.cellbiol.com/bioinformatics_web_development/ © cellbiol.com, all rights reserved

Figure 3 The comparison between the OSI Model and the TCP/IP Model[54]

However, the traditional OSI and TCP/IP models encounter their downfalls in pigeonholing and tackling cybercrimes. Building a crime resilient network system is beset and limited by the stereotypical reflection of cybersecurity from the armchair IT scholars who cleave to the notion that codes and technical devices play the

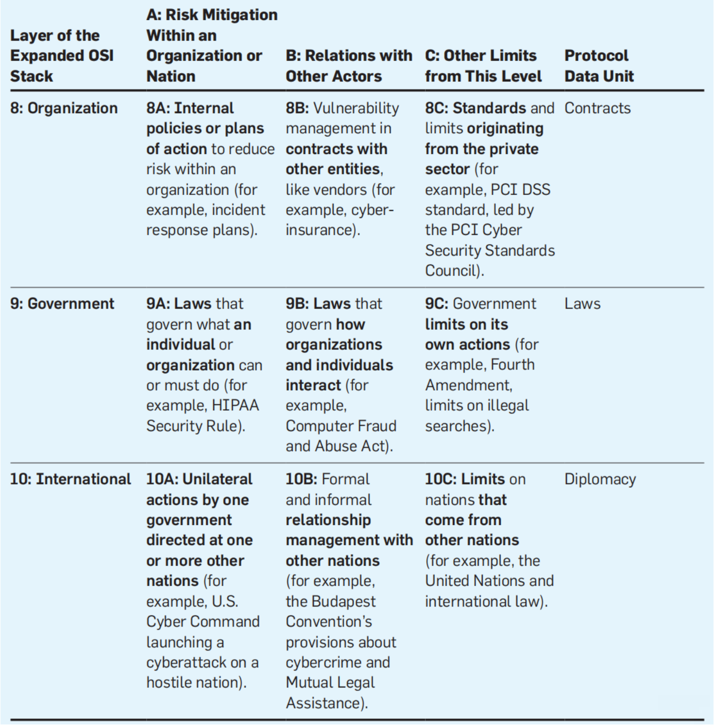
[54] Andrea Cabibbo, "Bioinformatics Web Development", cellibiol.com, chap1-2, accessed January 15, 2022, http://www.cellbiol.com/bioinformatics_web_development/.

defining actor in safeguarding network security. [55] In order to adapt the network governance to the wild evolution of IT technologies, the model should be extended to the non-code field that breeds risks and concerns of cybersecurity. [56] Carl Landwehr adds three more layers above the application layer as per the different scales of network users. [57] The eighth level will be the organizational layer where cybercrimes can take effect because of the poor management of the organizational cybersecurity system. The ninth layer rises from organizational routines to laws and legislatures. The vacancy or plagued spot of cybersecurity law legitimatizes the emerging cybercrimes, which aggravates the societal damage of cybercrimes. At last, the international society becomes the tenth layer of cybercrime. Since cyberspace exhibits anarchical features to some extent, diplomacy should regulate cyber activities and curb the spread of transnational cyber-based crime. The detailed analysis takes the form of a 3*3 matrix which is shown in Figure 3:

[55] Masike Malatji, Sune Von Solms, Annlizé, “Socio-technical systems cybersecurity framework,” *Information and Computer Security* 27, No.2(February 2019):233-272.

[56] Ibid.

[57] Peter Swire, “A Pedagogic Cybersecurity Framework,” *Communications of the ACM* 61, No.10 (October 2018): 23–26.



Layer of the Expanded OSI Stack	A: Risk Mitigation Within an Organization or Nation	B: Relations with Other Actors	C: Other Limits from This Level	Protocol Data Unit
8: Organization	**8A: Internal policies or plans of action** to reduce risk within an organization (for example, incident response plans).	**8B:** Vulnerability management in **contracts with other entities**, like vendors (for example, cyber-insurance).	**8C: Standards** and limits **originating from the private sector** (for example, PCI DSS standard, led by the PCI Cyber Security Standards Council).	Contracts
9: Government	**9A: Laws** that govern what **an individual** or **organization** can or must do (for example, HIPAA Security Rule).	**9B: Laws** that govern **how organizations and individuals interact** (for example, Computer Fraud and Abuse Act).	**9C:** Government **limits on its own actions** (for example, Fourth Amendment, limits on illegal searches).	Laws
10: International	**10A: Unilateral actions by one government directed at one or more other nations** (for example, U.S. Cyber Command launching a cyberattack on a hostile nation).	**10B:** Formal and informal **relationship management with other nations** (for example, the Budapest Convention's provisions about cybercrime and Mutual Legal Assistance).	**10C: Limits** on nations **that come from other nations** (for example, the United Nations and international law).	Diplomacy

Figure 3 The Matrix of the Added Layers and Their Components [58]

After knowing the holistic model of the internet, we are finally equipped with the paradigm to find the loopholes and crack the hidden security problems. The vulnerabilities that are subject to cyber-based crime vary and scatter through every layer of the network architecture. [59] Data breaches and cyberattacks are possible because every layer leaves vulnerable space for intervention and disruption. The protocols of each layer can also fail to counteract malicious cybercrimes. Thus, the model elaborated above gradually becomes a roadmap that helps the stakeholders define the emerging cybercrimes and issue systemic improvement on cyber security correspondingly.

c) Past Actions

The Open-Ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study of Cybercrime

[58] Ibid.

[59] Ibid.

The Twelfth United Nations Congress on Crime Prevention and Criminal Justice adopted the Salvador Declaration, which appeals to all Member States to advance their criminal justice and crime prevention system to keep up with the fast-changing world. In the declaration, member states eventually consented to jointly seek methods that can promote universal regulations to counter cybercrime[60] . And CCPCJ was invited by Congress to consider convoking an open-ended intergovernmental expert group to conduct a comprehensive study. Afterwards, the recommendation was adopted by CCPCJ, the United Nations Economic and Social Council (ECOSOC), and the General Assembly in the resolutions in sequence, and the first IEGmeeting took place in Vienna during January 17-21, 2011. [61&62] The meeting wrapped up with a specific methodology and timeline of combating cybercrime, and fully expounded the rights and obligations of relevant entities.

The Education for Justice (E4J) Initiative[63]

Adopted by the 13th United Nations Congress on Crime Prevention and Criminal Justice, the Doha Declaration emphasizes the significance of education in preventing crime and corruption. It also stresses the fundamentality in creating an

[60] UNODC, "Crime Congress wraps up with 'Salvador Declaration," United Nations Office on Drugs and Crimes, Jan. 15, 2022 accessed, https://www.unodc.org/unodc/en/frontpage/2010/April/crime-congress-wraps-up-with-salvador-declaration.html.

[61] UNODC, "Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime, 7th Session," United Nations Office on Drugs and Crime, Jan. 15, 2022 accessed, https://indico.un.org/event/1000086/.

[62] UNODC, "Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime," United Nations Office on Drugs and Crimes, Vienna, Jan. 15, 2022 accessed, https://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-jan-2011.html.

[63] "info sheet E4J EN," *United Nations Office on Drugs and Crimes,* Jan. 15, 2022 accessed, https://www.unodc.org/documents/e4j/flyers/info_sheet_E4J_EN_rev.pdf.

atmosphere that supports the rule of law, crime prevention and criminal justice by educating the younger generation in proper manners.

Under the Global Programme for the Implementation of the Doha Declaration, the Education for Justice (E4J) initiative constantly helps produce and spread educational information in the United Nations Office on Drugs and Crime (UNODC) mandated areas of crime prevention and criminal justice at all education levels. E4J provides freely-accessible online resources where instructors can learn and communicate through webinars and conduct their own researches.

II. Problems to be solved

a) Lack of All-Round Protection against Data Breaches

According to the explanation from the European Commission, data breaches happen when the data which should be safely managed for personal or organizational purposes becomes intently exposed so that individuals' personal information or organizations' confidential information come under high risks of illicit utilization.[64] The data breach has been one of the most notorious cybercrimes surging in recent years, already with an average business payment of $7.2 million per data breach back in 2010. [65] Data breach brings about massive financial loss and threats to privacy for sure, yet the reason why the aftermath of it can reach so high partly comes down to the recklessness of victims. Negligence of maintaining a fully-fledged protection system leaves plenty of room for data breaches to befall.

[64] European Commission, "what is a data breach and what do we have to do in case of a data breach," accessed January 19, 2022, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

[65] Dennis Tomlin, "Cyber security overview: prepare the worst so that we can be at our best," January 19, 2022 accessed, https://multco-web7-psh-files-usw2.s3-us-west-2.amazonaws.com/s3fs-public/IT%20Security%20Overview.pdf.

i. Absence of Precautionary Awareness

The means of an intended data breach has evolved rapidly since the age of information arrived. Back in the 1970s, data breaches only festered on the physical level, that is, stealing one's electronic devices or copying one's personal information with mobile storage devices like the USBs. Until these days, data breaches can occur on the application level demonstrated in the TCP/IP models. Deliberate hacking can directly target the interaction without being detected and countered. For so diversified and sneaky intended cyber breaches, the optimal way to satisfy the need for data protection is to strengthen the cyber defense system at the first step. [66]

Since data breaches become increasingly unpredictable, stakeholders encounter serious challenges in maintaining the data protection system against indiscriminate cyberattacks.

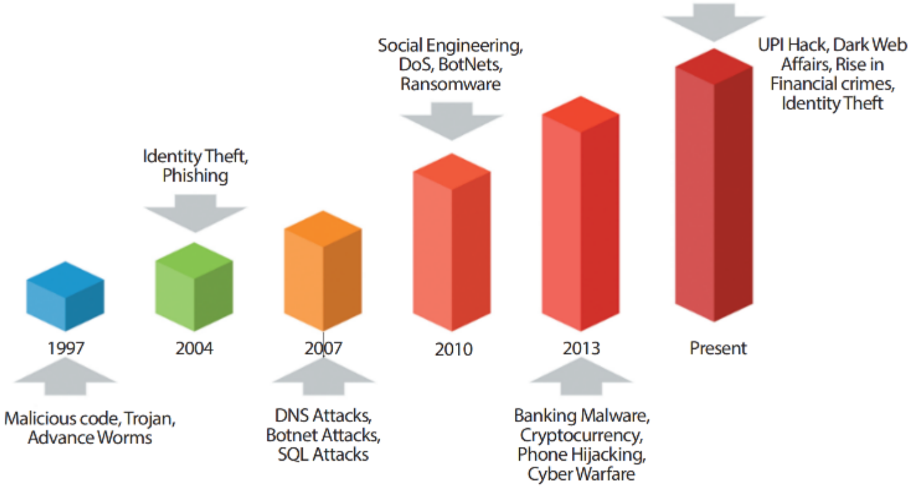

Social Engineering, DoS, BotNets, Ransomware
UPI Hack, Dark Web Affairs, Rise in Financial crimes, Identity Theft
Identity Theft, Phishing
1997
2004
2007
2010
2013
Present
Malicious code, Trojan, Advance Worms
DNS Attacks, Botnet Attacks, SQL Attacks
Banking Malware, Cryptocurrency, Phone Hijacking, Cyber Warfare

Figure 4 The Evolution of Data Breaches [67]

However, one major "dead zone" that makes precautionary protective measures hardly come in handy is the data users themselves and those who manage per-

[66] Chandra Sekhar Biswa, Subhendu Kumar Pani, "Cyber-Crime Prevention Methodology," In *Intelligent Data Analytics for Terror Threat Prediction*, eds S.K. Pani, S.K. Singh, L. Garg, R.B. Pachori and X. Zhang, 291-312.

[67] Ibid.

sonal data. Before individuals and organizations stumble upon data breaches, the natural fluke mind of "disasters will never go for me" keeps blinding them from proactively preparing necessary precautionary measures. In their paradigms, the awareness of taking precautionary measures doesn't constitute part of their habits.

Individuals are not habituated to the preventive mindset to avoid data breaches. They are more inclined to choose convenience over security in the delicate trade-off of cybersecurity.[68] For example, individuals are disposed to use the same old password everywhere, which is evidently subject to data losses. Also, they prefer to store their personal information in one virtual "nest" with no backup copies and always forget to update their data protection system provided by the vendors on their devices.

Organizations, especially SMEs that usually fall short of budget on data maintenance, are compelled by their Standard of Procedure(SoP), resulting in decision-makers leaving all the responsibility for data protection to the IT department and conferring limited power of data management to the executive employees.[69] Dereliction of concern over the state of the data protection system invariably increases the risk of data breach and aggravates the aftermath cost.[70] As shown in the graphic, the directors across businesses and charities in the UK still can't check their data protection system as frequently as they cover the paychecks.[71] Moreover, the person in charge of technical upgrades can be well undertrained. Lack of up-to-date information about the database and skills of immi-

[68] Matt Eddolls, "Making cybercrime prevention the highest priority," *Network Security,* Vol.2016, No.8(2016):5-8.

[69] Ibid.

[70] Ibid.

[71] "Cyber Security Breaches Survey 2021: Statistical Release," the Department for Digital, Culture, Media and Sport of the UK government, accessed January 20, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf.

nently responding to data breaches may wreak havoc on the technical precaution pack.

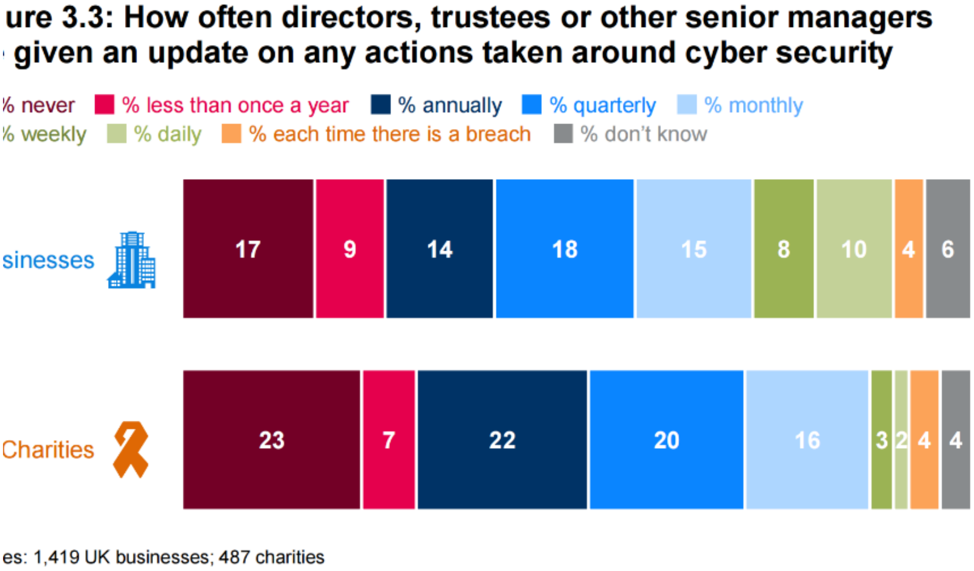


Figure 5 How often director trustees or other senior managers are given an update on any actions taken around cyber security[72]

In conclusion, from the perspective of subjects of whatever size, the absence of precautionary measures still plays a big part in minimizing the damage of data breaches.

ii. Increasing Technical Loopholes of the Information Protection System

In the TCP/IP model, there are exercising protocols that regulate online communication of data on every layer, and that's the part for pure network security. At technical perception, authentication indubitably sticks out as the fulcrum of data breach problems.

By definition, authentication denotes the proof process which ensures that the identity of the sender and recipient of the information shall be genuine. Concern-

[72] Ibid.

ing the result from the authentication, both two sides are to be checked in terms of their access to operating the data that comprise the message. [73]The Firewall is the most ubiquitous technology that carries out the mission.

However, standardized authentication can be easily broken down by various means. Attackers might acquire unauthenticated, remote access to the communication devices and adjust their data set points, which will obstruct timely warning to the communicators in the course of authentication. Apart from attacks targeting hardware, attackers might aim at the performance setting and the program design of the devices to inflict buffer overflow, which literally paralyze the authentication system with overdue amounts of codes in order to dysfunction the protection system and even take control of the functioning devices. [74] DoS attack is the most popular approach to bring about buffer overflow.

Besides, as comprehensive and regulatory as it may be, both the ARP on the network layer and the TCP on the transport layer have exposed their built-in flaws. The former protocol may cause confusion like network switches of the network devices because the ARP messages contain false MAC addresses, which will further initiate the physical breakdown of different scales.[75] The latter protocol can be aversely countered by injecting plenty of malformed packets under the cover so that the targeted devices shake off the operator's control or mistake the attackers with their original hosts, which is also known as IP spoofing.[76] If we track all the way to the application level, errors of the protocols are amplified by even more diversified individualized adversarial attempts. Session hijacking

[73] Tyler Moore, "The economics of cybersecurity: Principles and policy options," International Journal of Critical Infrastructure Protection, Vol.3, No.3-4(2010):103-117.

[74] Ibid.

[75] Glenn Surman, "Understanding Security Using the OSI Model," Sans Whitepaper, accessed January 20, 2022, https://www.sans.org/white-papers/377/.

[76] Chandra Sekhar Biswa, Subhendu Kumar Pani, "Cyber-Crime Prevention Methodology," In Intelligent Data Analytics for Terror Threat Prediction, eds S.K. Pani, S.K. Singh, L. Garg, R.B. Pachori and X. Zhang, 291-312.

aiming at predictable session tokens (also known as cookies) on the session level, cross-site scripting (XSS) attack that induce victims to access the malicious script uploaded into the webserver by the attackers on the presentation level, SQLi injection on the application level that fetches all the sensitive records in the database by obtaining a backdoor entry to the database and stealing user information constantly ever since, Trojans and viruses that ultimately manage to manipulate victims' network are all appendants to this category. [77]

When authentication systems break down, encryption becomes the last resort to keep the message private and intact throughout the conversation. Encryption includes algorithms and passwords, with the former complexifying the message on the transport layer and the latter exclusively abstracting message from the encryption by the users. Yet, both algorithms and passwords can be decoded by the attackers with the use of certain software or programs. The only way out for the network service stakeholders is to keep developing more complicated encryption algorithms in terms of logic, which demands higher theoretical R&D investment. The struggle there is that the cost to innovate more complex algorithms outclass the cost to crack down on the encryption on the transport level. To put it in a simpler way, the advancement of encryption is running a headwind race of time and money against data breaches.

For critical infrastructures and industries, after cracking down the network defense system, cyberattacks will creep into the Supervisory Control and Data Acquisition (SCADA) systems, where the collection and control of data take place. Since there are more processes vis-à-vis the IT data protection alone in an industrial network, timeliness, availability, integrity, confidentiality and degradation are all required.[78] In other words, the industrial network should respond to data breaches in time no matter which part of the

[77] Ibid.

[78] Bonnie Zhu, Anthony Joseph and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 380-388.

system fails. Also, they should utilize as many components of the SCADA system and guarantee normal functions as to data transmission, data generation, data storage and the overall payloads. [79] More than that, they should outpower the unauthorized intruders with a higher access level in hand. Knowing the attack has already affected the system, they should still manage to contain the damage within a tinted region lest the attacks should aggravate to a full-scale cascading data breach. Maintaining the defense line of the SCADA system in these five dimensions is always the core mission for enterprises to complete.

In brief, technical vulnerabilities of the data protection system have not been secrets, with people's familiarity with network architecture growing fast.

iii. Low Accessibility to Cyber Security Services

If the technical issues concern the vast majority who have a limited idea of the data protection mechanism, the users, whether they are individuals or organizations or official departments, will introduce the third-party cyber security service to make their data intact. From an ordinary individual's perspective, cyber security service indicates virus cleansing applications like McAfee and operation system updates. From an enterprise's perspective, cyber security service indicates cyber security companies sign service contracts with the enterprise to carry out regular checks and periodical renovation of the data protection system.

However, with growing demands for high-quality and high-frequency cyber security services, the payment for professional cyber security assistance holds high. [80] There are two reasons that can account for the low accessibility to cyber security services. First, entering the cyber security industry threshold is far higher than normal IT industries. The company in this industry should acquire not only valid

[79] Ibid.

[80] "2021 Cybersecurity Threats & Predictions," BKD Forensics Institute, accessed January 20, 2022, https://www.bkd.com/media/presentation-2021-cybersecurity-threats-predictions.

technical certificates to prove its capability but also heavy investments to support the maintenance of devices and watch out for the payroll. More than that, they should build up their credibility among their clients, which takes much capital and much time to earn a decent position for data protection always involve confidentiality, especially in the government branch. That accounts for the reason why there are merely a dozen of familiar cyber security service providers on the market wield the pricing power. Second, cyberattacks are launched as accidents in the eye of the victims. Without the knowledge of the exact time data breach will fall and cost data breach will bring, the trade-off between convenience and security again tips over in favor of convenience. Paying for fixing a structural problem ingrained in the data protection system at a costly price seems an uneconomical option to either individuals or organizations compared to post-hoc data recovery and cyberattack attribution.

b) Malicious Impingement against Privacy

i. Rampant Acts of Individual Hackers and Hacker Groups

Usually, cyber-crimes can be ascribed to the criminal acts of hacker groups. In the process of data breaches and cyberattacks, they station themselves in the middle of users and their destination servers, as illustrated in Figure 6.[81] Although sporadic hackers sometimes attack other network users' connections and devices out of personal sentiments, they usually hack for economic and political benefits. What seems more horrendous is that the hacker groups have already grown big enough to make hacking an industry astride the grey zone of law.

[81] Geeks for Geeks, "How to prevent Man in the Middle Attack," accessed Jan. 21th, 2022, https://www.geeksforgeeks.org/how-to-prevent-man-in-the-middle-attack/.

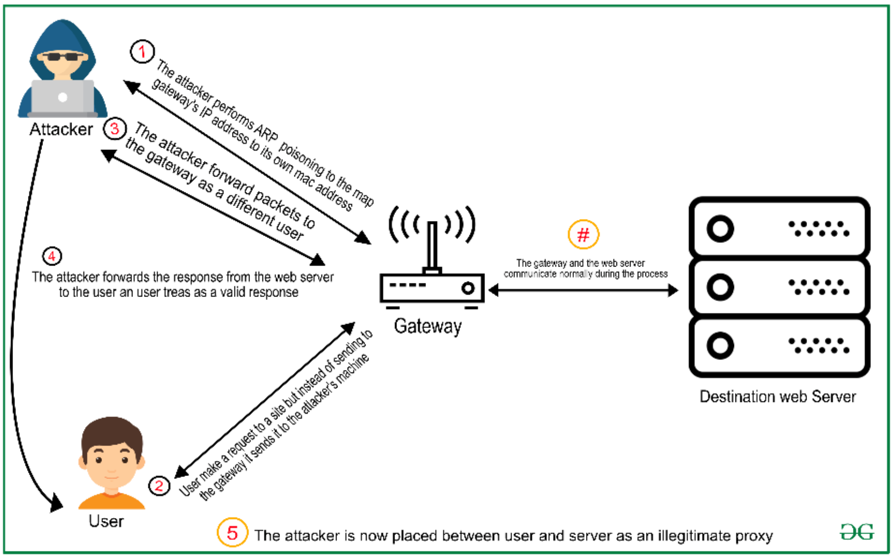

Attacker
① The attacker performs ARP poisoning to the map gateway's IP address to its own mac address
③ The attacker forward packets to the gateway as a different user
④ The attacker forwards the response from the web server to the user an user treas as a valid response
Gateway
# The gateway and the web server communicate normally during the process
Destination web Server
② User make a request to a site but instead of sending to the gateway it sends it to the attacker's machine
User
⑤ The attacker is now placed between user and server as an illegitimate proxy

Figure 6 Display of the Man-in-the-Middle (MITM) Cyber Attack Model [82]

Since the world ushers into the age of information, hacker groups spontaneously loom as a constant indicator of cybercrimes. However, the criminal acts of hacker groups are still hard to contain. Hacker groups practicing hacking activities that lead to severe economic and social impact are doomed to being detected, tracked and facing legal charges, whereas minor ones are successfully hidden in the piles of cyberattacks lawsuits.

There are four major premises that undergird the criminal motive of hacker groups and add the difficulty of strict law enforcement against them.

First and foremost, the technical caliber of hacker groups adds their possibility to avoid leaving evident forensic traces online, which gets them out of the official supervisors' focus. Compared with the entry threshold of the cyber security industry, hacking group members are usually daft and swift at identifying encryption and running their malicious codes to operate the targeted data flow. Furthermore, hacker groups have a clear division of tasks to crack down on a single data pro-

[82] Ibid.

tection system. With specialization and process control, the hacker groups can instantly orchestrate cyberattacks aiming at the weak points under cover of fake identity or normal portal connection, whereas the victim side can hardly degrade the damage and collect server entry information simultaneously.

Second, the hacker groups pay less cost than the victims for a round of cyberattacks. Since hacker groups attack from the dark, their ad hoc calculation will make sure they can optimize the overall expense. To say the least, even if the hacker groups fail at their attempts, they only waste the preparation cost because they are free of bound in terms of responsibility for others compared to the victims. Furthermore, the expected cost for legal punishment remains at a low level if the cyberattacks are not directed at highly confidential information in business or politics. [83]

Third, hacker groups feature their anonymity. Unlike in the real-time society where one person is tagged with countable identities, hackers can acquire multiple digital identities to confuse the law enforcers along the forensics process. Even if the digital identities get revealed through searching the attacked system's access log, there is still a long way to go for the law enforcers to trace hackers' real identifications from digital identities and other virtual adversarial sources. The hackers can easily camouflage their IP addresses and Mac addresses with the help of VPNs. Also, hacker groups are in the air of opportunism. They usually intend to launch attacks at the right timing that can distract cybercrime issues from other societal prolems, especially in a time of natural disasters. [84] For instance, there were certain hacker groups faking donation websites and cracking down personal bank

[83] Matt Eddolls, "Making cybercrime prevention the highest priority," *Network Security*, no.8(2016):5-8.

[84] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple and Xavier Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security,* no.15(2021).

accounts right after Hurricane Katrina hit the east coast of America.[85] Furthermore, one of the most significant inherent loopholes of the TCP/IP protocol leaves sufficient room for hackers to hide their identities. The whole protocol is mainly destination-oriented and receiver-oriented, which can be interpreted as a lack of standards regulating senders of information. Hackers can easily and persistently exploit this loophole to orchestrate relentless cyberattacks.

Fourth, hacker groups enjoy plenty of resources to underpin their successful hackings. In other words, the hacker groups can also access the cyber security expertise, official white book on data protection, the errors of data protection technologies publicized via social media and the cut-edge encryption models, having adequate knowledge of the current state of affairs of cyber security if no more than normal network users. All those open social resources and public releases ultimately serve the hackers in a way and become redirected against the people that those publications are originally designed to protect.[86] Moreover, the hacker groups exchange information with each other instead of keeping away from each other. They not only share crucial information on the defense systems but also share their "weapons", e.g., malware, viruses and strategies, which strengthen the potential destructive ability of each hack group.

Last but not least, there are hacker conglomerates that operate for their own political pursuit and economic benefits, yet there are still a vast number of hacker groups asked to launch cyberattacks. The mounting demands for cyberattacks, in fact, propel the hacking groups to form a hacking market and even a hacking industry. The economic interaction between hacker groups and their clients further justifies cybercrimes and leverage latent social resources to facilitate the development of the hacking industry.

[85] Ibid.

[86] Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, Vol.38, No.1-2(2015):4-37.

ii. State-operated Espionage

Espionage is variably politicized for the crime suspects move from individual and corporate bodies to nation-states. The government body's interest in cyber security is akin to a flip of a coin: on the one hand, the government should strengthen its legitimacy by safeguarding the indispensable right of liberty; on the other hand, the government should also be obliged to monitor the cyberspace and collect data for the overall security of the society. From the standpoint of government bodies, the anarchical propensity of cyberspace carries unpredictable risks that might give rise to their downfall. Thus, it is convinced that the government bodies should maximize their reach of personal information within the tacit boundary that determines whether the rights of the civil society are respected or not.

In the field of international law, opinions about the legality of state-operated espionage still vary. Some contend that espionage and cyber-surveillance should be considered as the natural outreach within the jurisdiction of intelligent departments, an inalienable part of a nation's duty. They can wield the right to access first-hand personal information or acquire them by hiring hacking proxies for the sake of national security. [87] Others diametrically oppose the view and contend that nation-states are obliged to prioritize the privacy of individuals, or hacking activities may derive justification for their criminal acts from states' practices. [88] Controversial as it may be, espionage between states is a common and rather traditional

[87] Katharina Ziolkowski, "Peacetime Cyber Espionage-New Tendencies in Public International Law," In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013),425-64.

[88] Dinah PoKempner, "Cyberspace and State Obligations in the Area of Human Rights,"In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013), 239-60.

activity that is an internationally accepted state practice. [89] Snowden's confession of the Prism Program initiated by the National Security Agency (NSA) in the USA reveals a tip of an iceberg. [90] The intelligence agency intended to monitor what individuals want by turning to search engines and how they describe their lives via social media by launching such programs.

The more horrible aftermath inflicted by national cyber espionage is the escalation of cyberwar and the change of power. The most representative example comes down to US's cyberattacks against Iran's nuclear strategy with Stuxnet. [91] Also, there is abundant evidence of how governments eavesdrop on opposing activists' dialogues with surveillance devices to crack down on potential uprisings. [92]

State cyber espionage is similar to a hidden trigger to national conflicts in the age of information. Thus, how to contain the impact of cyber espionage should be a major topic included as the extreme form of cybercrimes.

iii. Case Study: The Far-Reaching Impacts of WikiLeaks Evince a Revolutionary Change in Global Digital Order

[89] Katharina Ziolkowski, “Peacetime Cyber Espionage-New Tendencies in Public International Law," In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013), 425-64.

[90] Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian,* June 6,2013, http://www.theguardian.com/world/2013/jun/06/ustechgiantsnsadata.

[91] Katharina Ziolkowski, “General Principles of International Law as Applicable in Cyberspace," In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013),135-88.

[92] Oliver Leistert, “Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts," *Surveillance and Society*, vol.9, no.4(2012): 441-56.

The ambivalence of which the government partakes on national security illustrates how complex the essence of cybercrimes can be and how intractable the problems of the existing digital order can be. This controversial uncertainty eventually got amplified with the advent of Hacktivism represented by the notoriously renowned hacker group WikiLeaks. The big questions have surfaced ever since: should the government hide all the classified information from the populace? Is it legit for network users around the world to emancipate the hidden brute truth by hacking activities, wielding the inalienable Right to Know for the sake of Freedom of Information (FoI)?[93]

The prime time of WikiLeaks at which the hacking group came to the spotlight was in 2010 when they disclosed the Collateral Murder video, the Afghan War Diaries, the Iraq War logs and the US diplomatic cables, all of which were released to question the official propagated justification of the US military. [94] As the world witnessed, Julian Assange, the leading role of WikiLeaks, became an imputed international felon and went under after nearly a decade of boycott from internet service providers like Google and financial sources like the Swiss Bank.[95] The retaliation against WikiLeaks wound up successfully with Julian Assange being shackled from the Ecuador embassy after years of diplomatic asylum.

But before the information strife signalled by WikiLeaks' exposition of Pentagon documents into a global incident, the hacking organization had already deeply engaged in politics. Back in 2007, one year after WikiLeaks registered its domain name, they re-

[93] Yochai Benkler, "A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate," *Harvard Civil Rights-civil Liberties Law Review*, vol.46(), no.2(2011): 331-397.

[94] Alasdair Roberts, "WikiLeaks: the illusion of transparency," *International Review of Administrative Sciences,* vol.78, no.1(2012):116-133.

[95] Yochai Benkler, "A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate," *Harvard Civil Rights-civil Liberties Law Review,* vol.46(), no.2(2011): 331-397.

leased two classified documents pertinent to Africa, revealing the intended assassination planned by the rebel leader of Somalia and the ingrained corruption by the incumbent Kenyan leader. [96] In the same year, WikiLeaks started investigating the political environment of the US by exposing the details of the Guantanamo Bay detention camp.[97] Since then, the hacking organization not only went further on the investigation into the US's Middle-East records and the blemishes of the superpower's political figure, including Senator Sarah Palin, who was the candidate for Vice President with the republican John Sidney McCain. Nonetheless, strangely and ironically, WikiLeaks once even received the Amnesty International's New Media Award, an honor that was regarded as the most meritorious liberal media in the eyes of the bureaucrats from Europe and the US.

Like a meteorite streaking across the international society, their omnipresence within a very short period caused massive impacts on the political landscape, showing the reason why a hacking community can earn such leverage and breath a new life into attributing cybercrimes. Unlike traditional revolutionaries driven by a sense of anarchy, the organizational structure of WikiLeaks took on a decentralized form. With merely 40 core members and 800 volunteers scattered across the world, the hackers operated coordinately, simply on account of them being rallied under the creed “all information should be free” and “protecting the whistleblowers”.[98] However, the opt-outs of key members like “the Architect” and Domscheit-Berg led to the personification of WikiLeaks, which impaired public support with the icon Julian Assange himself attacked relentlessly by the authorities. [99]Besides,

[96] Bart Cammaerts, “Networked Resistance: The Case of WikiLeaks,” *Journal of Computer-Mediated Communication,* vol.18, no.4(2013): 420-436.

[97] Ibid.

[98] Peter Ludlow, “WikiLeaks and Hacktivist Culture,” the Nation, Accessed February 8, 2022, https://www.thenation.com/article/archive/wikileaks-and-hacktivist-culture/.

[99] Bart Cammaerts, “Networked Resistance: The Case of WikiLeaks,” *Journal of Computer-Mediated Communication*, vol.18, no.4(2013): 420-436.

WikiLeaks well capitalized on the social capital throughout its movement. After noticing the deficiency in spreading their achievements, Julian Assange reached out to other hacking communities like Anonymous, one of the most enduring hacking groups that feature its battle against the Church of Scientology and its creation of Tor-related encrypted proxy-servers, and traditional media including the Guardian, the New York Times and Der Spiegel. [100&101] The enormous "revelation network" undergirded the formidable force of activism.

Hacking communities are usually observed to be villainous through the lens of universal values. Hacking activities are indubitably inflicting serious data breaches. They are seen to disrupt national security for their personal propensity and debase national interest at the cost of individual privacy. However, Hacktivism, born in the anarchical atmosphere of cyberspace, has garnered more and more proponents in its crusade against secrecy and the legitimacy of state operations. [102] The rise of Hacktivism deserves a second thought of the nation-states. Instead of blindly snuffing out them, countries are obliged to rebuild the Government to Citizen (G2C) channels to better adapt to the age of information.

iv. Unrestricted Commercialization of Personal Information

As there are overt cybercrimes like cyberattacks, there are also illegal trades of data behind the scene where service suppliers, marketers and advertisers intend to transgress personal information security in exchange for an expected swell on corporate revenues.

[100] Karin Whal-Jorgensen, 'Is WikiLeaks Challenging the Paradigm of Journalism? Boundary Work and Beyond," *International Journal of Communication,* vol.8(2014): 1-12.

[101] Mark Coddington, "Defending a Paradigm by Patrolling a Boundary: Two Global Newspapers' Approach to WikiLeaks," *Journalism & Mass Communication Quarterly,* vol.89, no.3(2012): 377-396.

[102] Jessica L. Beyer, "The emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party and Iceland," *Journal of Computer-Mediated Communication*, vol.19, no.2(2014):141-154.

In the light of the critics from political economy, the metabolism of the market in cyberspace still pertains to the rule of value and the four stages of commodity circulation. In an interactive relationship between a network user and an online service supplier, before the user is permitted to access the service, they should all acquiesce in the "User Agreement", the underlying fact beneath which reveals the inequity between the user and the supplier. [103] Users exchange their personal information like ID numbers, bank accounts, family addresses for the supplier's provision of network services. In fact, the ostensibly equal transaction paves the way for the corporations to valorize the data, to further realize its value, and to exploit more benefits exclusive to themselves. This interaction also enables the corporations to cultivate a sense of fear for "losing out" in the consumers so that they are compelled and willing to sacrifice their private information.[104] These senses aggregate and form an incorrigible cognitive culture of the consumers, which shows how coercive the power of the corporations can be.

Apart from corporations' power play to make users' personal information profitable, the advent of big data takes a stride beyond. Consumers leave traces from which their private information can be deducted, and the corporations consequentially acquire peoples' data with the massive statistical power of big data. Thanks to the algorithms of big data, the concept of Panopticon coined by Bentham that conceives of a glass-wall prison with no hiding place for each prisoner has come to life in the cyber world. [105] Thanks to the detrimental side of big data technology, the commodification of personal information has already been assimilated endogenously to the partnership among the unicorn internet enterprises. The cooperation between Cambridge Analytica and Facebook evince in-depth that the commodification of personal information may produce profound political

[103] George R.Milne, Andrew J.Rohm, and Shalini Bahl, "Consumers' Protection of Online Privacy and Identity," *Journal of Consumer Affairs*, vol.38, no.2(2004): 217-32.

[104] John Edward Campbell and Matt Carlson, "Panopticon.com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media*, vol.46, nno.4(2002): 586-606.

[105] Ibid.

clout that fortifies the interdependence between internet giants and motivates the micro cartel to keep capitalizing on their advantage vis-à-vis the individual consumers. [106]

c) Ill-Conditioned Cyber Community

A crime-resilient network system doesn't only indicate the overall protection against cyber-dependent criminal acts but cyber-enabled criminal acts as well. The most defining trait of the internet is that cyberspace is not just a platform rather a medium that molds a virtual society based on online interactions. The cyber community transcends above the organic paradigm of the internet. The circulation of the cyber community closely correlates with reality. The change of the cyber community may amplify the change of reality or counteract the change of reality. Cybercrimes pertain to this principle without a shadow of a doubt, which shapes cybercrimes to be much more complex.

[106] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian,* March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

i. Dissemination of Disinformation

Information can be regarded as the predominant element that constitutes the cyber community. However, there is still heated debate over the legal status of disinformation. According to the definition, disinformation denotes false, inaccurate, or misleading information designed, presented and promoted to deliberately inflict public harm or for profit.[107]

The main reason why disinformation can diffuse over the whole cyber community is that the identities of purveyors of disinformation usually vary in terms of scale and power. Political actors like politicians, political parties and interest groups may have the motive to fabricate provoking messages to get their values across.[108] Besides, media doesn't entail professionalism and independent journalism. Vested in them the freedom of media legitimatized by the constitution, they can intentionally produce disinformation on certain events to manipulate societal attention and public opinions. [109]Moreover, the network users may produce disinformation on the basis of their subjective views via social media. The flaws of incomplete civil society forged by anti-intellectualism and extremism get amplified because of the fast transmission speed of data, which ultimately make disinformation widespread.[110] The cyber community enables all the network stakeholders to wield their right of speech to achieve their own goals, yet fails to prescribe the right of speech, which feeds the extension of the anarchical part of the cyber community.

Apart from the diversified subjects and their hardly limited capacity to disseminate opin-

[107] "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation," the European Commission, accessed January 21, 2022, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en#_publicationDetails_PublicationDetailsPortlet_relatedPublications.

[108] Ibid.

[109] Ibid.

[110] Ibid.

ions, the impact of disinformation can be even more intractable. Disinformation will go to two ends after all: one is ideological conflict; the other is defamation. That accounts for the reason why hate speeches and conspiracy theories usually originate from disinformation today. The insanity of disinformation can be fuelled by the internet, and the reasoning part of network users' minds can be put through the binary question of rights and wrongs. As a result, the disinformation infiltrates the crowd and subjects its divisive power to them with the help of the cyber community.

ii. Unregulated Circulation of Cryptocurrency

The fervour of cryptocurrency emerged in the latest decades. As nascent as it may be, the cryptocurrency has already fit right in the global finance market. For the cyber communities, the emergence of it emanates a huge revolution that will determinately change the dynamic of cyberspace.

The currency itself is created on the basis of blockchain technology which adopts a multi-nodes system to enhance the authenticity of information and the safety of users' privacy.[111] Underpinned by the bolstering effect on cyber security of the blockchain technology, cryptocurrency is embedded with unrestrainable economic power that puts itself onto a controversial spot.

Economically speaking, the rocketing value of cryptocurrency poses a serious challenge to fiat currency. For speculators and opportunists who intend to rip some gains off the rippling wave of cryptocurrency, many of them regard it as a blue-chip financial product and choose to overweight all forms of cryptocurrency, such as bitcoin and dogecoin. As we know, one of the most important monetary functions is to realize exchange among commodities as a universal equivalent. Since there are surging trades and transactions dealing with cryptocurrency, this new type of currency whose value is denominated only by digital mining and marketing hype would be capable of igniting a full-scale financial

[111] Shiv Hari Tewari, "Abuses of blockchain and Cryptocurrency in dark web and how to regulate them," EasyChair Preprints 4995(February 2021).

crisis and destabilizing the international economy if it should not be regulated carefully.[112]

From the perspective of legal status, the stance on cryptocurrency still varies from country to country. However, the fact that cryptocurrency can level cybercrime up to a more sophisticated level should not be neglected. On account of its confidentiality and credibility, cryptocurrency has become a custom liquidity unit in the dark web markets where illegal trades of drugs are orchestrated, and vulnerable groups are undergoing horrible exploitation. [113] The law enforcers find it hard to trace cryptocurrency flow and further obtain little forensic evidence in imputation. Moreover, by the nature of cryptocurrency, financial crimes have crept into cyberspace and extended to this new form of currency. Thanks to its crypticity, money laundering and unapproved gambling get to stealthily exist in cyberspace and poison the cyber community. [114]

All in all, cryptocurrency can be a significant trigger to stimulate the evolution of cyber-enabled crimes and increase the difficulty of combating them.

iii. Catalyst of an Expanding Crime Network

Cyberspace sets up so interactive and convenient a cyber-community that even organized criminal groups adapt their routines to the dynamic of the internet. Criminal organizational bodies like gangs and terrorists, shall we say, have become successfully incorporated into cyberspace and the era of information. Although they still carry out their illicit conduct offline, criminal groups increasingly depend on the internet for the sake

[112] John Fry and Eng-Tuck Cheah, "Negative bubbles and shocks in cryptocurrency markets," *International Review of Financial Analysis 47*(October 2016): 343-52.

[113] George Hurlburt, "Shining Light on the Dark Web," *Computer*, Vol.50, No.04(2017):100-105.

[114] Raffaella Barone and Donato Masciandaro, "Cryptocurrency or usury? Crime and alternative money laundering techniques," *European Journal of Law and Economics 47*(February 2021):233-54.

of convenient conversation. While the internet reveals these groups out of the darkness and dissolves the traditional structure within the groups, the internet also contributively helps with their recruitment, their publicity and their influence.[115] Thus, the criminal groups enlist more young jobless network users and expand their influential territory. Also, the internet enhances their propensity to create delinquencies and accentuates their identity as gangsters or official members of terrorist groups. [116] Encouraged by the stereotypical impression of them, the criminals are more likely to post intimidating videos and malicious messages online to live up to their negative expectations. Moreover, the internet makes their criminal strategy more fragmented in cyberspace than in offline neighbourhoods. Normally, the online initiated by them are rather campaigns reflecting symbolic objectives. Under the guidance of universal pursuit and the calling of collective identities, they can maintain and even strengthen the coordination of the groups where they belong. Meanwhile, the internet enables them to diffuse responsibility and conduct crimes independently with the communicative function of the internet, which will catalyze the transformation of the criminal groups that render them higher flexibility and more tactical resources. [117] As a result, the cyber groups will still evolve from the offline realities to cyberspace and keep endangering the authority and the society by forming a transboundary crime network.

[115] David C. Pyrooz, Scott H. Decker and Richard K. Moule Jr., "Criminal and Routine Activities in Online Settings: Hangs, Offenders, and the Internet," *Justice Quarterly*(March 2013):1-29.

[116] Ibid.

[117] Manuel R. Torres Soriano, "The Vulnerabilities of Online Terrorism," *Studies in Conflict & Terrorism*, vol.35, no.4(June 2013): 263-77.

III. Possible Solutions

a) Improving the Data Protection Mechanism from Every Link[118]

i. Early Identification and Detection of Potential Attacks

With the increase of internet penetration rate, there is an exponential growth of all kinds of links between computers. The computer systems have become more complex over time. To attackers that are well versed in intrusions, complex systems, such as Multi-interface virtual real-time operating systems on the Windows platform, mean more underlying vulnerabilities. [119]The more complex the system is, the easier it is for intruders to detect, lurk, attack and retreat, and the more likely it is for the users of the service to suffer greater losses.

Therefore, detection of potential attacks beforehand becomes particularly critical. One solution is to set up attack warning mechanisms, but early warning gradually fails to counter the fast-evolving offenses carried out in better-organized and more efficient ways. The key to establishing a suitable detecting mechanism is to build a comprehensive defense system that operates according to the specific situation of the defense target and integrates the warning system with defense measures. Besides, given the constant upgrade of attack approaches, virus databases should be updated regularly to maximize protection against the emergence of "super viruses" and "virus resonances" (the situation where two viruses interact with each other and cause much greater damage than they

[118] Dan Klinedinst, “Coordinated Vulnerability Disclosure”, Software Engineering Institute, Carnegie Mellon University, https://resources.sei.cmu.edu/asset_files/Webinar/2016_018_101_465576.pdf.

[119] Yuxin, Wang, “Design and Implementation of Multi-interface Virtual Real-time Operating System on Windows Platform”, accessed Feb 9, 2022. https://xueshu.baidu.com/usercenter/paper/show?paperid=1x6q0tv0w42e0c10646e0am0w0416991.

are separated).

ii. Response and Recovery at the Post-Incident Stage

No defense system can prevent all attacks. Once an intruder has caused substantial damage, the primary goal of the defending party is to minimize the damage. Firstly, service providers are obliged to inform their users of ways to avoid potential attacks and the appropriate stop-loss measures in case they are attacked. Secondly, service providers should fix the vulnerability by immediately releasing patches to prevent further attacks. Finally, users should pay close attention to the latest progress of the event and take measures such as cutting off the network connections to protect their information security when appropriate.

At the same time, users may use a system log to check why errors occur or to look for traces left by attackers. Moreover, Network backup is an efficient way to save routine business records as files. However, more attention should be paid to DNS registration information on the network system to locate the information leaks and possibly the hacker. It is also vital to contain the adverse impacts of information leakage to a certain degree. "Stopping the leakage" is, from time to time, more urgent than catching cybercriminals, since the priority should be minimizing damage.

The cooperation of private sectors, government, and, most importantly, service providers is required for quick response and recovery. Various actions need to be taken to prevent re-occurring of similar attacks. Defense systems such as firewalls should be strengthened; service providers should upgrade their systems, and users should cautiously protect their personal information.

iii. Raising Public Awareness of Protecting Cyber Security (Skill Training, habituation)

With the popularization of personal computers (PC), Internet users are increasing rapidly. But the vast majority of today's Internet users have received little specific skill training, which may bring great challenge to the whole information security system. For one thing, some Internet users with low awareness of information security are likely to contribute to network offenses unknowingly. Taking advantage of these people's bad habits when surfing the internet (i.e., always turning hot spots on or using free Wi-Fi networks provided at hotels and cafes), intruders can easily acquire access to a specific network or a puppet machine for launching large-scale offenses. For another, network users proficient with computer technology may ignore the provisions of international network conventions and cybercriminal laws to launch attacks on other computers or computer systems.

In order to improve the public awareness of information security, the government may encourage all units, enterprises and schools to carry out information security education, such as courses and lectures of relevant legal knowledge. Network intrusion attack and defense simulation contests or relevant demonstrations can be carried out in innovative forms such as live broadcasting to show the possible attack modes of potential network attacks, losses caused, and corresponding preventive measures.

b) Adapting Existing Governance Paradigm to the Dynamic of Cyberspace

i. Propelling the Application of Adequate Network Authentication Process

Network Authentication is the process that verifies the user's identification to a network service to which the user is trying to gain access. [120] As a fundamental procedure for information-protection in both public and private domain, network authentication is the first line of defense against cybercrime. However, challenges

[120] ScienceDirect, "Network Authentication", *ScienceDirect,* Jan. 19, 2022 accessed, https://www.sciencedirect.com/topics/computer-science/network-authentication

including Trojan-horse, adversarial jammers, unauthorized modification or application of information, etc., are faced by the ever-evolving cyberspace.

To start with, VPNs are a major part of the information technology landscape since it connects remote users and offices. Systematic approaches have been taken to ensure cyber security. For pass-through authentication, secret key cryptography and limited access to the user's password have reduced the risk of Trojan horse and protected the database. As for information packets, corruptions might be committed by jammers. At the same time, either they can be detected and discarded by internal nodes or their influences can be eliminated by the inherent linear coding structure of end-to-end authentication. IDs and passwords are essential to network authentication as well.

The application of adequate network authentication processes need to propelled. A more convenient, simplified, and efficient authentication system is expected to be built around the globe. From the users' side (e.g., passwords, choice of server) to the inherent structure of the internet (e.g., TCP-IP) to the providers' side (e.g., Microsoft Windows, IOS,) a comprehensive and co-operating system for authentication need to be established.

ii. Facilitating the Coordination of Online and Offline Operation

Cybercrime, by definition, takes place in the online world. However, both cybercriminals and their electronic devices are objective beings in the physical world.

Coordinating efforts online with operations offline stands for a critical shift in the entire process of law enforcement. For example, we may locate the user's IP on the net through network lines. At the same time, possibilities remain that the target device with identified IP may be intentionally damaged and therefore unable to locate, or the user is actually remotely controlling the device, and therefore insufficient information is provided for arresting the criminal.

As for the Internet of Things, hackers can remotely control or hijack devices and thus cause security threats to hardware devices, communication, mobile application, etc. Its governance may introduce more specific practical scenarios, i.e., Smart City Scenario, to guard the offline side through onlinesimulation. [121]

With the Internet as the carrier, pyramid selling intertwined with financial fraud displays an expanding trend. Raising public awareness is crucial to both preventing the expansion of criminal gangs and reducing the incidence of fraud. Online and offline actions need to be taken in both raising public awareness (including propaganda films, posters, online discussion boards, etc.,) and tackling cybercrime. [122]

When it comes to transborder cybercrime, the cooperation of local police under bilateral or multilateral agreements or international assistance is also vital to an efficient operation. International Criminal Police Organization (INTERPOL) has created a platform for mutual assistance in transborder cybercrime that focuses on joint action among national police departments offline. [123] Online operation may bring about offline acts and vice versa. Either way, the coordination between them is essential for cyberspace governance.

iii. Strengthening Emergency Response to Cyber Crises

Due to the instantaneity of network information transmission, emergency response is an important factor in addressing cyber crises. Immediately after hackers breached through firewalls, personal information could be leaked, an industry could collapse, and even national security could be at risk. Meanwhile, a timely and effective response can reduce the scope of adverse outcomes.

[121] Yuan, Fan, “New Security in the Era of Convergence and Innovation", *Informatization Construction*, May, 2018, page 22-24

[122] China Security Certificate Research and Development Center, “Online and Offline Joint Management of ‘Prevention, Control, and Fight’ combined", *China Anti-Counterfeiting Report*, Nov, 2017

[123] INTERPOL, “What is INTERPOL", *International Criminal Police Organization*, Jan.11, 2022 accessed, https://www.interpol.int/Who-we-are/What-is-INTERPOL

As for the procedural emergency response, the severity of the crime may determine the complexity of the process. When it comes to cross-border cybercrimes that demand mutual assistance, the requesting Party may request to order or obtain expeditious preservation of stored computer data after showing the intention to submit a request without literally sending any formal request. [124] This can reduce the approval process and improve efficiency. At the same time, serious crimes require strict procedures. Extradition is usually met based on dual criminality and applicable extradition treaties.

As for prevention and "rehearsal" of the emergency, contingency tests are also influential. In the meantime, such tests should be operated on proportionate standards and scales. They should be properly assessed in order to offer reliable instruction when an emergent response is required in real life.

As for remediation and reconstruction, different data storage models such as distributed and parallel databases call for different responses, and the capability of the original security system also influences post-crisis actions. For example, after information leakage, the most urgent task is to eliminate the wider transmission of related information. And the first thing to do after being hacked is to cut off the part under attack from its connected partners. A comprehensive and detailed action-response guidebook could be written beforehand to reduce time searching for solutions, contribute to cyber security, and offer insights into the prevention of future crimes. [125]

c) Securing Legal Utilization of Personal Information in the Private Sector

i. Stimulating the Development of Cyber Security Service Enterprises

[124] Council of Europe, "Budapest Convention", *Council of Europe*, Nov.23, 2001, Article 29

[125] CIO, "Ten Things You Must Do after Being Attacked by Hackers", *CIO,* Jul. 8, 2015 accessed, http://blog.sina.com.cn/s/blog_6f50ebbb0102w22e.html。

Cyberattacks are evolving in two directions nowadays. Through encrypted communication, intruders around the world may organize and launch widely distributed specialized and targeted attacks. Besides, Internet attacks are becoming more industrialized, which means people with intentions to commit cybercrimes are able to obtain "services" that target specific individuals or organizations more easily. Since the cost of defense far outstrips that of offense, most service providers cannot defend themselves against massive cyberattacks.

These problems explain the urgent demand in the organizations that provide corresponding defense systems. Capable enterprises should be encouraged to develop enhanced defense systems against cyberattacks and set up sub-units to provide cyber security services to the public.

Governments should launch policies that encourage the development and installment of defense systems, such as tax breaks, fiscal subsidies and relaxation of financing limits. At the same time, VPNs and information processing of government offices must be rightful, legitimate and controllable. Otherwise, confidential information could be leaked, which may jeopardize national and public security. For example, Mrs. Clinton's use of private email accounts and private servers for official business during her tenure as Secretary of State is not considered a proper way to handle government secrets.

ii. Promoting the Regulation of User Data Transfer among Enterprises

In recent years, Internet users' personal information can be leaked due to profiteering or malicious attacks on enterprise networks. For one thing, the relevant personnel in charge are often ignorant about or disregard information security; For another, loopholes may exist in the confidentiality agreements among users and service providers and the agreements on circulating users' information among enterprises. One solution is to improve the Protection Measures for the Circulation of Personal Information. This approach is not limited to private enterprises. However, it should emphasize the obligations of private enterprises when obtaining personal information from other departments or organizations, especially other private enterprises. The penalties imposed if violating relevant regulations should also be underlined. Government departments may also consider setting up expert groups that work with private sectors and related stakeholders to develop and improve guidelines for Internet crime prevention. Regulations on data transfer among enterprises and advocacy could be included, providing useful guidance for individuals and organizations to prevent cybercrimes.

iii. Clarifying Terms of Service with Users

Though some enterprises have taken the lead in clarifying Terms of Service with their users recently, legislation and law enforcement must also follow up if the problem of excessive collection of personal information is to be solved. In view of the relatively long legislative process, member countries can first guide enterprises to improve the User Service Terms set under the existing laws and regulations by improving the reward and punishment mechanism. And disciplinary measures including interviews, inquiries and fines can be imposed on the enterprises unwilling to observe the rules. With respect to the enterprises that refuse to make corrections after repeated reminders, necessary coercive measures may be taken following relevant laws and regulations.

Enhancing personal data governance models is also a method to solve the inequality in terms. Compared to individual-style data governance and state-style data governance, a collective data governance model is a better choice. Data trust is just one type of collective data governance model that realizes algorithmic counteraction through bottom-up group autonomy and can effectively deal with inequality in the data economy. [126]

[126] Fengling, Ding, "Selection of Personal Data Governance Models: Individual, Nation or Collective", *Journal of Huazhong University of Science and Technology (Social Science Edition),* Nov 9, 2021. https://d.wanfangdata.com.cn/periodical/hzkjdxxb-shkxb202101010.

Country Position

a) USA

The United States is the main birthplace of Internet technology and the country with the most widespread Internet application. Ensuring cybersecurity has become one of the primary problems in the United States. From Clinton, Bush, Obama, and Trump, the information security policy of the United States has gradually matured through the process of proposing, detailing, systemizing, and internationalizing. In recent years, the aim of the US's information security policy has developed from singly enhancing national network security to competing for strategic advantages in the field of cyberspace at the same time.

First of all, the United States builds the "troika" of information security institutions and puts forward the concept of "cyber deterrence" to implement active defense. The United States is building a system of strike, penetration and defense capabilities in cyberspace, which has been centered around the NSA, CIA and Homeland Security.

Second, the United States has placed a special emphasis on public-private partnerships and information sharing. Defense Advanced Research Projects Agency (DARPA) has cooperated with an American company to develop Zero-Knowledge Proof technology to promote trusted computing and encryption. [127]

Thirdly, the US has sped up the training of cyber security personnel and enhanced the public's awareness of cyber security.

In addition, the United States is one of the first countries in the world to initiate active cyberattacks so far, and the National Security Agency has initiated the formation of the

[127] Zhenjing, Li, "DARPA Asked an American Company to Use Zero-Knowledge Proof Technology to Promote Trusted Computing and Encryption", *China National Defense Science and Technology Information Center,* Feb. 8, 2022 accessed, https://www.sohu.com/a/395443221_313834

world's largest cyber warfare force. [128]

In the field of international cooperation, although the Budapest Convention was not written by the United States, America still has a first-mover advantage in making rules against cybercrime. The dominant position of the United States in the Internet field has been continuously consolidated. At the same time, the US is supportive of global cyberspace governance based on the Budapest Convention.

On the other hand, during the pandemic, illegal activities such as selling Covid-19 vaccines, fake vaccination cards, and fake nucleic acid negative proof are taking place on the "dark web". A fake vaccination card is sold on the "dark web" at 150 dollars, using cryptocurrency such as Bitcoin. [129]

b) Russia

Russia is one of the first countries to regulate Internet activities. Even though it has suffered from malicious cyber-attacks from other countries, after years of development and improvement, Russia has gradually revealed its operational capability in the field of network governance, completely reversing its previous passive backwardness.

Russia builds an effective network security protection mechanism in the following aspects. To start with, raising cyber security to a strategic level and establishing a legal and regulatory system for network information security. Furthermore, building a multi-tiered network security guarantee system. Last but not least, improving the overall technical advantage in network security. Russia refused to sign the Budapest Convention, which came

[128] Anshujun, "A Comparison of Chinese and American Network Security Strategies", *Anshujun,* Jan. 28, 2022 accessed, http://zhuanlan.zhihu.com/p/61982089

[129] Know Chuangyu Cloud Security, " A 'Dark Web' in the United States has Revealed Fake Covid-19 Markets to Guard Against Theft of Personal Vaccine Information", *Know Chuangyu Cloud Security,* Feb. 8, 2022 accessed, https://xw.qq.com/cmsid/20210604A08ZHW00

into force in 2004 for the reason that its clauses are too intrusive. [130]

At the same time, Russia's Hydra "dark web" market has become a hot spot for illegal activity, attracting $1.37 billion worth of cryptocurrencies in 2020, up from $9.4 million in 2016. The annual surge in transactions meant that the Hydra "dark web" market grew 624% year-on-year from 2018 to 2020. [131] Numerous actions have also been taken by the Russian Federation to encounter cybercrime committed on and\or via "dark web". Russia's Federal Security Service (FSB) said it had cut off one of Russia's biggest drug smuggling channels and its sales through the "dark web" on September 24, 2021. [132]

As for global operation, Russia has been pushing for a new United Nations treaty to govern cyberspace since 2017. In terms of cybercrime convention and governance, the Russian government publicly announced in early December 2019 that it had successfully completed the external "disconnection" test exercise of the national Internet, just one month after the enactment and application of the Internet Sovereignty Law of the Russian Federation on November 1, 2019. This can effectively eliminate the infringement and threat from other countries and international networks.

[130] Computer and Network Security, "Analysis of Russian network security", *Computer and Network Security,* Jan. 24, 2022 accessed, https://www.sohu.com/a/237011646_653604

[131] Cnbeta, "Russia's Hydra Dark Wed made more than 1.3 billion Dollars Last Year", *Cnbeta,* Feb. 9, 2022 accessed, https://www.chinaz.com/2021/0527/1256345.shtml

[132] Interface News, "Russia's Federal Security Service (FSB) Has Shut down 'Dark Web' Drug Distribution Channels", *Interface News*, Nov. 24, 2021,

c) European Union

The Budapest Convention is written by the European Union and serves as the most widely-acknowledged framework for global cooperation on cybercrime. But with the continuous development of cyberspace, the Budapest Convention faced some challenges. And EU has been strengthening its cyber technology sovereignty and leadership by all means.

The following aspects are highlighted in the strategic planning of the European Union's network security construction in the next ten years. Cyber sovereignty: attaching importance to the sovereignty of cyberspace and enhancing EU's cyber resilience; Cyber norms: Emphasizing legislation, setting up Cyber Security Action Center (SOCs), and creating Joint Cyber Unit; Personnel training; Deepen cooperation: deepening cooperation with partners and stakeholders, upholding global leadership, and promoting a global open and secured cyberspace. [133]

Through its European Cyber Crime Centre (C3), Europol has been actively monitoring the dark Web for years and helped to take down some large dark web marketplaces, such as AlphaBay.[134] And in 2018, European Union authorities have seized $5.2m worth of cryptocurrencies in a drug bust against "dark web" sellers. [135]

As a regional political and economic organization, the EU is still faced with many problems, such as the democratic deficit, identity crisis and low decision-making effectiveness. There are also some inherent problems with its cybersecurity policies, including difficul-

[133] Interface News, "Russia's Federal Security Service (FSB) Has Shut down 'Dark Web' Drug Distribution Channels", *Interface News*, Nov. 24, 2021,

[134] Jun, Ni, "EU Law Enforcement Agencies Join Forces to Tackle down Dark Web Crime", Feb. 9, 2022 accessed, https://xueshu.baidu.com/usercenter/paper/show?paperid=1g0r0rb0ht4e0480fc0g0220nk115420&site=xueshu_se

[135] Ming, Yi, "EU Cracks down on 'Dark Web' Drug Sellers, Seizing 5.2 Million Dollars in Cryptocurrency", Jun. 29, 2018, http://www.bianews.com/news/details?id=15295&type=0

ties in regional coordination and excessive politicization.

d) China

China has become a great power in the digital space, but it still faces many challenges. For one thing, though China is one of the few countries whose overall ICT capabilities match those of the United States, there are technological gaps between China and developed countries, led by the US, in high-end chip manufacturing, industrial software design and system software development. For example, since there is no computer system independently developed by Chinese, most of the China's institutions and departments have to install various versions of Windows on their computers. While these groups pay High annual patent fees to Microsoft, their computers are likely to be affected if the virus spreads on a large scale, as was the case with the leak of Eternal Blue, the NSA's hacking weapon.

For another, China has been plagued by Cyber-Enabled Crimes such as telecom fraud in recent years. In six months of 2019, China's public security organs solved 118,000 telecom and Internet fraud cases and arrested 99,000 suspects. [136] In 2020, 256,000 cases were solved, and 263,000 suspects were arrested. [137] In the first 11 months of 2021, 370,000 cases were solved, and 549,000 suspects were arrested. [138] Thanks to the rapid development of digital communication systems and their numerous loopholes, telecom fraud is increasingly rampant and has become one of the major crimes plaguing the Chinese gov-

[136] "Carry out full-chain Strikes -- China cracks down on Telecom and Internet fraud," The Ministry of Public Security of the People's Republic of China, Accessed Feb 9, 2022. https://www.mps.gov.cn/n2255079/n6865805/n6865942/n6865949/c6872689/content.html.

[137] "China's public security organs cracked 256,000 cases of telecom and Internet fraud in 2020," The Ministry of Public Security of the People's Republic of China, Accessed Feb 9, 2022. https://app.mps.gov.cn/gdnps/pc/content.jsp?id=7633791.

[138] China Police Daily, "More than 370,000 cases solved, number continued to decrease," *China Police Daily,* CN11-0090, Jan 1, 2022. http://epaper.cpd.com.cn/szb/wwwcpd_9/dzb_16465/rmga/2022/2022_01_01/16466_2022_01_01_29110/.

ernment and the public.

In face of the harsh reality, China took actions both internationally and domestically. On the multilateral scale, China is actively promoting consensus on the harmless and efficient use of ICT. In the 12th BRICS forum, China underlines "the importance of an open, secure, stable, non-discriminatory, accessible and peaceful ICT environment" and calls on BRICS countries to "work together to develop common approaches to data security to promote prosperity and inclusive growth". [139] On the domestic scale, China has been polishing its own legal system. On June 1, 2017, The Cybersecurity Law of the People's Republic of China came into effect, [140] giving the relevant departments direct law enforcement basis in dealing with criminal cases. On September 1 and November 1, 2021, the Data Security Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China, which had long been called for by the civil and academic world, took effect respectively. [141&142] These laws illustrate the strengthening of China's ability and determination in cracking down on cybercrimes.

[139] "Recommendations of the 12th BRICS Academic Forum to the Leaders: BRICS New Vision for a Better World (Clause 16)," BRICS Academic Forum, Accessed Jan 25, 2022. https://brics-russia2020.ru/images/106/14/1061406.pdf.

[140] "Order of the President of the People's Republic of China: Number 53," Jinping Xi, Accessed Jan 25, 2022. http://www.npc.gov.cn/npc/c12488/201611/4fedbbd187cc4764890b212097ee584f.shtml.

[141] "Data Security Law of the People's Republic of China," xinhuanet, Accessed Jan 25, 2022. http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.

[142] "Personal Information Protection Law of the People's Republic of China," The National People's Congress of the People's Public of China, Accessed Jan 25, 2022. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

e) African Union [143]

Due to the underdevelopment of African countries as a whole, the African Union (AU) needs the support of non-regional countries in most cases when dealing with the major issues related to regional development. Most AU countries are not capable enough in countering cybercrime due to their inability to maintain their own Internet sovereignty. Some African countries with stable internet access are often engaged in bitter struggles with Western media groups to control the development of public opinion (as is the case in Egypt during the Arab Spring of 2011), while many other African countries are insufficiently supplied with internet infrastructures. This kind of inability, which is mostly the reflection of the government's inability to maintain steady economic growth and stable political environment, is one of the major reasons that help explain why African countries often fall victim to fast-evolving Cyber-Enabled Crimes. The large majority of African countries busy tackling coups, demonstrations and economic failure are easy targets for criminals and transnational criminal groups. These countries are often caught off guard when being offended, and usually they are not able enough to reach out to the criminals that launch the offenses, be it Cyber-Dependent Crimes or Cyber-Enabled Crimes.

Besides, the power struggles among the major African countries over the decades proved to be a hindrance to a possible agreement. Despite AU's effort to forge a regional consensus on cybersecurity and personal information protection in recent years, there has been little response. On June 27, 2014, the African Union Convention on Cyber Security and Personal Data Protection was adopted by the general assembly, but the document still only has 8 ratifications and 14 signatories after Angola acceded on February 21, 2020. [144] Overall, the cybersecurity efforts in African countries are often outweighed by the de-

[143] 29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)

[144] "List of countries which have signed, ratified/acceded to the African Union Convention

mand in other fundamental areas such as alleviation of poverty, and this imbalanced situation was exacerbated by the COVID-19 pandemic.

on Cyber Security and Personal Data Protection."African Union, Accessed Jan 25, 2022. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

Questions to Consider

1.Who are the stakeholders of cybercrime prevention? How do you categorize them?

2.Try to describe the interactions between cyberspace and other spheres (e.g. economy, finance, politics, etc.) and how they may affect countries and individual stakeholders.

3.In which aspects did the Internet contribute to transforming (or to some extent, exacerbating) criminal activities in the information era?

4.Why are some governments unwilling to cooperate in global operations against cybercrime? And what are their major concerns?

5.What criteria did we use in this Background Guide to categorize different cybercrime? What are the two main categories of cybercrime in our discussion?

6.What is the most influential protocol on cybercrime? And why did certain countries like China and Russia refuse to sign it?

7.Are cyber forces a necessity for countries in this increasingly digitalized world? Why or why not?

8.Do you think the current network architecture is responsible for the spread of terrorism and the expansion of criminal territories? How come?

9.Network users can hardly protect their privacy against the prying attempts orchestrated by internet tycoons and state bodies. On that score, how can we finesse internet governance to maintain the balance between individual privacy, commercial profit and national cyber security?

10.As effective as it functions, the OSI model is ingrained with technical loopholes that lean upon serious cybercrime. From both strategic and pragmatic perspectives, what the internet operators can do to push safety and stability of the internet to the next level?

Bibliography

African Union. “AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.” African Union, Jan. 21, 2022 accessed. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

African Union. “LIST OF COUNTRIES WHICH HAVE SIGNED, RATIFIED/ACCEDED TO THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.” African Union, Jan. 18, 2022 accessed https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

An, Shujun. “A Comparison of Chinese and American Network Security Strategies”. Zhihu.com, Jan. 28, 2022 accessed. http://zhuanlan.zhihu.com/p/61982089.

Auxier, Brook. “Children's Engagement with Certain Types of Digital Devices Varies Widely by Age.” Pew Research Center, Jul. 28, 2020. Feb. 10, 2022 accessed. https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/.

Raffaella, Barone, Masciandaro. Donato. “Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques.” European Journal of Law and Economics vol.47. Feb, 2021. p233-54.

Yochai, Benkler. “A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate.” Harvard Civil Rights-civil Liberties Law Review, vol.46. no.2(2011): 331-397.

L. Beyer, Jessica. “The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party and Iceland.” Journal of Computer-Mediated Communication, vol.19. no.2(2014):141-154.

Biswa, Chandra Sekhar Subhendu Kumar Pani. “Cyber-Crime Prevention Methodology.” Intelligent Data Analytics for Terror Threat Prediction, eds S.K. Pani. S.K. Singh. L. Garg. R.B. Pachori and X. Zhang. 291-312.

BKD Forensics Institute. "2021 Cybersecurity Threats & Predictions." BKD Forensics Institute, Jan. 20, 2022 accessed. https://www.bkd.com/media/presentation-2021-cybersecurity-threats-predictions.

Bossler, Adam M. and Tamar, Berenblum. 2019. “Introduction: New Directions In Cybercrime Research." Journal of Crime and Justice, vol.42 (5): 495-499.

BRICS Academic Forum. “RECOMMENDATIONS OF THE 12TH BRICS ACADEMIC FORUM TO THE LEADERS: BRICS NEW VISION FOR A BETTER WORLD.” BRICS Academic Forum, Dec. 26, 2021 accessed. https://brics-russia2020.ru/images/106/14/1061406.pdf.

Britannica. “Double Criminality”. Britannica, Jan. 14, 2022 accessed. https://www.britannica.com/topic/double-criminality.

Brooks, Chuck. “3 Key Cybersecurity Trends to Know for 2021 (and On...)”. Forbes. Apr. 12. 2021. Jan. 11. 2021 accessed. https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/?sh=77782cc49786.

Carole, Cadwalladr, Graham-Harrison. Emma. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” The Guardian, Mar.17, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cammaerts, Bart. “Networked Resistance: The Case of WikiLeaks.” Journal of Computer-Mediated Communication, vol.18, no.4(2013): 420-436.

John Edward, Campbell, Carlson. Matt. “Panopticon.com: Online Surveillance and the Commodification of Privacy.” Journal of Broadcasting & Electronic Media, vol.46, no.4(2002): 586-606.

CCPCJ. “New and Emerging Forms of Crime: Threats the World Must Reckon With”. 13th United Nations Congress on Crime Prevention and Criminal Justice, Apr. 2015. Feb. 11, 2022 accessed. https://www.un.org/en/events/crimecongress2015/pdf/Factsheet_5_Emerging_forms_of_crime_EN.pdf.

CCPCJ. “Report of the Open-Ended Intergovernmental Expert Group on the Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States. the International Community and the Private Sector”. ECOSOC, Apr. 11-15. 2011. Jan. 13. 2022 accessed. https://documents-dds-ny.un.org/doc/UNDOC/GEN/V11/803/26/PDF/V1180326.pdf?OpenElement.

China Police Daily. “More Than 370,000 Cases Solved, Number Continued to Decrease.” China Police Daily, CN11-0090. Jan 1, 2022 accessed. http://epaper.cpd.com.cn/szb/wwwcpd_9/dzb_16465/rmga/2022/2022_01_01/16466_2022_01_01_29110/.

China Security Certificate Research and Development Center. “Online and Offline Joint Management of ‘Prevention, Control, and Fight’ combined”. China Anti-Counterfeiting Report, Nov. 2017.

CIO. “Ten Things You Must Do after Being Attacked by Hackers.” CIO, Jul. 8, 2015. http://blog.sina.com.cn/s/blog_6f50ebbb0102w22e.html.

Clinton, Larry, Dobrygowski, Daniel, Joyce, Sean, and Friso Van der Oord. “Principles For Board Governance Of Cyber Risk.” Insight Report, Geneva: World Economic Forum. 2021. Jan. 10, 2022 accessed. https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.

Cnbeta. “Russia's Hydra Dark Wed made more than 1.3 billion Dollars Last Year”. Cnbeta, Feb. 9, 2022 accessed. https://www.chinaz.com/2021/0527/1256345.shtml.

Coddington, Mark. “Defending a Paradigm by Patrolling a Boundary: Two Global Newspapers' Approach to WikiLeaks.” Journalism & Mass Communication Quarterly, vol.89, no.3(2012): 377-396.

Computer and Network Security. “Analysis of Russian Network Security.” Souhu.com, Jan. 24, 2022 accessed. https://www.sohu.com/a/237011646_653604.

Council of Europe. “Actions Against Cybercrime.” Council of Europe, Feb. 7, 2022 accessed. https://www.coe.int/en/web/cybercrime/home.

Council of Europe. “Convention on Cybercrime.” European Treaty Series. Nov. 23, 2001.

Council of Europe. “Council of Europe and Eurojust Joint Workshop on International Cooperation in Cybercrime: Joint Investigation Teams/Joint Investigations”. Council of Europe Portal, Oct. 2021. Jan. 21. 2022 accessed. https://www.coe.int/en/web/cybercrime/council-of-europe-and-eurojust-2021-annual-meeting-jits#{%22107800064%22:[0]}.

Council of Europe. “Explanatory Report to the Convention on Cybercrime”. European Treaty Series, 23. Nov. 2001.

Council of Europe. “The Budapest Convention on Cybercrime: benefits and impact in practice”. T-CY. Published 13. Jul. 2020

Council of the European Union. “Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade”. Council of the European Union, Mar. 9. 2021

Daniel, Goldstein, Hogan-Burney, Manky. 2020. “Partnership against Cybercrime.” Insight Report. Geneva: World Economic Forum, Jan. 17, 2022 accessed. https://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf.

Ding, Fengling. “Selection of Personal Data Governance Models: Individual, Nation or Collective”. Journal of Huazhong University of Science and Technology (Social Science Edition), Nov 9, 2021. https://d.wanfangdata.com.cn/periodical/hzkjdxxb-shkxb202101010.

Djordjevic, Nikola. “The Elderly and the World Wide Web”. MedAlertHelp.org, Jan.5, 2022. Feb. 10, 2022 accessed. https://medalerthelp.org/blog/elderly-the-world-wide-web-infographic/#:~:text=And%2C%20when%20it%20comes%20to%20the%20Internet%2C%20age,Internet%20usage%20to%20three%20or%20five%20times%20weekly.

ECOSOC. “Implementation of General Assembly Resolution 46/153 Concerning Operational Activities and Coordination in the Field of Crime Prevention and Criminal Justice.” ECOSOC, Jul. 30, 1992. https://www.unodc.org/documents/commissions/CCPCJ/ECOSOC_Resolution-1992-22_E.pdf.

Eddolls, Matt. “Making Cybercrime Prevention the Highest Priority.” Network Security, vol.2016. No.8(2016):5-8.

European Commission. "What is a Data Breach and What Do We Have to Do in Case of a Data Breach.” European Commission, Jan. 19, 2022 accessed. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

F. Lipson. Howard. “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy”. Carnegie Mellon Software Engineering Institute, Nov. 2002. Jan. 14. 2022 accessed. https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf.

Fan, Yuan. “New Security in the Era of Convergence and Innovation.” Informatization Construction, May. 2018. p22-24.

Fry. John, Eng-Tuck Cheah. “Negative Bubbles and Shocks in Cryptocurrency Markets.” International Review of Financial Analysis, vol. 47(October 2016): 343-52.

Geeks for Geeks. “How to Prevent Man in the Middle Attack.” Geeks for Geeks, Jan. 21, 2022 accessed. https://www.geeksforgeeks.org/how-to-prevent-man-in-the-middle-attack/.

General Assembly. “Creation of an Effective United Nations Crime Prevention and Criminal Justice Programme.” General Assembly Resolution, A/RES/46/152 (18 December 1991). https://www.unodc.org/documents/commissions/CCPCJ/GA_Resolution-46-152_E.pdf.

Gibson Miralis, Nyman. “International Cross-border Cybercrime Investigations: Recent Developments”. Lexology.com, Jan. 10, 2019. Feb. 11, 2022 accessed. https://www.lexology.com/library/detail.aspx?g=29aa9398-dd82-49b1-b48f-43586dc6e0e6.

GI-TOC. “Strategy 2021-2023”. Global Initiative Against Transnational Organized Crime.” GI-TOC, Jan. 2021.

Global Initiative against Transnational Organized Crime. “Strategy 2021-2023.” Global Initiative against Transnational Organized Crime, Jan. 2021. https://globalinitiative.net/wp-content/uploads/2021/02/GI-TOC-Strategy-2021-2023.pdf.

Greenwald, Glenn and MacAskill, Ewen. "NSA Prism Program Taps in to User Data of Apple, Google and Others.” The Guardian, Jun. 6, 2013. http://www.theguardian.com/world/2013/jun/06/ustechgiantsnsadata.

Hurlburt, George. “Shining Light on the Dark Web.” Computer, vol.50, no.04(2017):100-105.

Interface News. “Russia’s Federal Security Service (FSB) Has Shut down ‘Dark Web’ Drug Distribution Channels”. Interface News, Nov. 24. 2021. https://baijiahao.baidu.com/s?id=1711768793767577966&wfr=spider&for=pc.

INTERPOL. “Cybercrime Collaboration Services”. International Criminal Police Organization, Nov. 2020

INTERPOL. “National Cybercrime Strategy Guidebook”. International Criminal Police Organization, Apr. 2021.

INTERPOL. “What is INTERPOL.” International Criminal Police Organization, Jan.11, 2022 accessed. https://www.interpol.int/Who-we-are/What-is-INTERPOL.

Johnson, Joseph. “Global Internet Access Rate 2005-2019.” Statista, Jan. 27. 2021. Jan. 12. 2022 accessed. https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since-2006/.

Klinedinst, Dan. “Coordinated Vulnerability Disclosure.” Software Engineering Institute of the Carnegie Mellon University, Dec. 11, 2021. https://resources.sei.cmu.edu/asset_files/Webinar/2016_018_101_465576.pdf.

Know Chuangyu Cloud Security. “A ‘Dark Web’ in the United States has Revealed Fake Covid-19 Markets to Guard Against Theft of Personal Vaccine Information”. Know Chuangyu Cloud Security, Feb. 8. 2022 accessed. https://xw.qq.com/cmsid/20210604A08ZHW00.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple and Xavier Bellekens, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," Computers & Security, no.15(2021).

Lasse Lueth. Knud. "State of the IoT 2020: 12 Billion IoT Connections. Surpassing Non-IoT for the First Time". IoT Analytics, Nov. 19. 2020. Jan. 11. 2022 accessed. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

Leister, Oliver, "Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts." Surveillance and Society, Vol.9, No.4(2012): 441-56.

Leukfeldt, E. R. "The offline side of cybercrime: Mapping involvement mechanisms in cybercriminal networks". Dec. 2021. https://www.nwo.nl/onderzoek-en-resultaten/onderzoeksprojecten/i/93/29793.html.

Li, Zhenjing. "DARPA Asked an American Company to Use Zero-Knowledge Proof Technology to Promote Trusted Computing and Encryption". China National Defense Science and Technology Information Center, Feb. 8, 2022 accessed. https://www.sohu.com/a/395443221_313834.

Ludlow, Peter. "WikiLeaks and Hacktivist Culture." The Nation, February 8, 2022 accessed. https://www.thenation.com/article/archive/wikileaks-and-hacktivist-culture/.

Milne, George R., Andrew J.Rohm, and Shalini Bahl, "Consumers' Protection of Online Privacy and Identity." Journal of Consumer Affairs, Vol.38, No.2(2004): 217-32.

Miniwatts Marketing Group. "Internet World Penetration Rates by Geographic Regions – 2021." Internet World Stats, Jan. 16, 2022 accessed. https://www.internetworldstats.com/stats.htm.

Moore, Tyler. "The economics of cybersecurity: Principles and policy options," Internationalal Journal of Critical Infrastructure Protection, vol.3, no.3-4(2010):103-117.

Morgan, Steve. "The World Will Store 200 Zettabytes of Data by 2025". Cybercrime Magazine, Jun.8. 2020. Jan. 15. 2022 accessed. https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/.

Ni. Jun, "EU Law Enforcement Agencies Join Forces to Tackle down Dark Web Crime". Feb. 9. 2022 accessed. https://xueshu.baidu.com/usercenter/paper/show?paperid=1g0r0r-b0ht4e0480fc0g0220nk115420&site=xueshu_se.

Souza, Nicole de. "The Nth Room Case and Modern Slavery in the Digital Space". The Interpreter. Jan. 13. 2022 accessed. https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space.

Pei, Wei. 2021. "Public-Private Cooperation In Cross-Border Combat Against Cybercrime." Information Security And Communications Privacy 7: 37-45.

Pei. Wei. "Law Enforcement Jurisdiction in Cross-border Data Forensics of Cybercrime". Study of Comparative law. Feb. 7. 2022 accessed. http://www.360doc.com/content/21/1231/14/72442254_1011276322.shtml

PoKempner, Dinah. "Cyberspace and State Obligations in the Area of Human Rights." In Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, edited by Katharina Ziolkowski, 239-60. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013.

Pyrooz, David C., Scott H. Decker and Richard K. Moule Jr.. "Criminal and Routine Activities in Online Settings: Hangs, Offenders, and the Internet." Justice Quarterly (March 2013):1-29.

Qi, Wu. "Jurisdiction Conflicts and Resolutions in Cyberspace". Journal of Southwest University of Political Science & Law, vol. 23, no. 1: 48-49.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks,” Journal of Strategic Studies, vol.38, no.1-2(2015):4-37.

Roberts, Alasdair. “WikiLeaks: the illusion of transparency.” International Review of Administrative Sciences, vol.78, no.1(2012):116-133.

Rogers, M. Everett. "The Internet and Sustainable Development". UNESCO-Encyclopedia Of Life Support Systems (EOLSS) II. Accessed Jan 21, 2022. https://www.eolss.net/ebooklib/sc_cart.aspx?File=E6-33-03-05.

ScienceDirect. “Network Authentication.” ScienceDirect. Jan. 19. 2022 accessed. https://www.sciencedirect.com/topics/computer-science/network-authentication

Soriano, Manuel R. Torres. “The Vulnerabilities of Online Terrorism.” Studies in Conflict & Terrorism, vol.35, no.4(June 2013): 263-77.

Surman, Glenn. “Understanding Security Using the OSI Model.” Sans Whitepaper. Accessed January 20, 2022. https://www.sans.org/white-papers/377/.

Tewari, Shiv Hari. “Abuses of blockchain and Cryptocurrency in dark web and how to regulate them.” EasyChair Preprints 4995(February 2021).

The Department for Digital, Culture, Media and Sport of the UK government. "Cyber Security Breaches Survey 2021: Statistical Release.” The Department for Digital, Culture, Media and Sport of the UK government. Accessed January 20, 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf.

UNODC. “The Doha Declaration on integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation." "UNODC. Accessed Jan 24, 2022. https://www.unodc.org/res/ji/import/international_standards/doha_declaration/doha_declaration.pdf.

The European Commission. "A multi-dimensional approach to disinformation: Report of the independent High-Level Group on fake news and online disinformation." The European Commission. Accessed January 21, 2022. https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en#_publicationDetails_PublicationDetailsPortlet_relatedPublications.

The Ministry of Public Security of the People's Republic of China. "Carry out full-chain Strikes -- China cracks down on Telecom and Internet fraud." Accessed Feb 9, 2022. https://www.mps.gov.cn/n2255079/n6865805/n6865942/n6865949/c6872689/content.html.

The Ministry of Public Security of the People's Republic of China. "China's public security organs cracked 256,000 cases of telecom and Internet fraud in 2020." Accessed Feb 9, 2022. https://app.mps.gov.cn/gdnps/pc/content.jsp?id=7633791.

Tomlin, Dennis. "Cyber security overview: prepare the worst so that we can be at our best." Accessed January 19, 2022,.https://multco-web7-psh-files-usw2.s3-us-west-2.amazonaws.com/s3fs-public/IT%20Security%20Overview.pdf.

United Nations Office on Drugs and Crime (UNODC). "Around The World in Three Ccpcjs: Muns Tackle SDG16." UNODC. Accessed Jan. 15, 2022. https://www.unodc.org/doha-declaration/en/news/2019/02/around-the-world-in-three-ccpcj.html.

United Nations Office on Drugs and Crime (UNODC). "The Commission On Crime Prevention And Criminal Justice." UNODC. Accessed Jan. 13, 2022. https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html.

United Nations Office on Drugs and Crimes. “Crime Congress wraps up with 'Salvador Declaration." UNODC. Accessed Jan 20, 2022. https://www.unodc.org/unodc/en/frontpage/2010/April/crime-congress-wraps-up-with-salvador-declaration.html.

United Nations Office on Drugs and Crimes. “info sheet E4J EN." Accessed Jan 19, 2022. https://www.unodc.org/documents/e4j/flyers/info_sheet_E4J_EN_rev.pdf.

United Nations Office on Drugs and Crimes. “Microsoft Word - Methodology timeline REV-7.doc." Accessed January 22, 2022. https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Working_Papers/Methodology_timeline_REV-7.pdf.

United Nations Office on Drugs and Crimes. “Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, 7th session." Accessed Nov 8, 2021. https://indico.un.org/event/1000086/.

United Nations Office on Drugs and Crimes. “Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime." Accessed January 21, 2022. https://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-jan-2011.html.

United Nations Office on Drugs and Crimes. “University Module Series: Cybercrime." Accessed Dec 16, 2021. https://www.unodc.org/e4j/en/tertiary/cybercrime.html.

United Nations. “The New Normal Is Digital”. Department of Economic and Social Affairs. Accessed Jan. 9, 2022. https://www.un.org/en/desa/new-normal-digital.

United Nations. “Peace, Justice and Strong Institutions - United Nations Sustainable Development." 2022. United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/peace-justice/.

University Module Series Cybercrime. “Module 7 International Cooperation Against Cybercrime." UNODC. Feb. 11. 2022 accessed. https://www.unodc.org/e4j/en/cybercrime/module-7/index.html.

UNODC. "Comprehensive Study on Cybercrime." UNODC. Accessed Feb 3, 2022. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC. "Cybercrime Repository." United Nations Office on Drugs and Crime. Accessed Jan. 19. 2022. https://www.unodc.org/unodc/es/cybercrime/cybercrime-repository.html.

UNODC. "Cybersecurity Measures and Usability." UNODC. Jan. 13. 2022 accessed. https://www.unodc.org/e4j/en/cybercrime/module-9/key-issues/cybersecurity-measures-and-usability.html.

UNODC. "National Capacity and International Cooperation." UNODC. Jan. 15. 2022 accessed. https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/national-capacity-and-international-cooperation.html.

UNODC. "Report on the Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime Held in Vienna from 27 to 29 July 2020." UNODC. Accessed Jan 18, 2022. https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/UNODC_CCPCJ_EG.4_2020_2/UNODC_CCPCJ_EG.4_2020_2_E.pdf.

Viano, Emilio C. "Cybercrime: Definition, Typology, and Criminalization." In Cybercrime, Organized Crime, and Societal Responses. Switzerland: Springer International Publishing, 2017.

Hagy, David W. "Electronic Crime Scene Investigation: A Guide for First Responders. Second Edition," U.S. National Institute of Justice. Jan. 15. 2022 accessed. https://www.ojp.gov/pdffiles1/nij/219941.pdf.

Walker, Summer, and Ian Tennant. “Control, alt, or delete? The UN cybercrime debate enters a new phase.” Global Initiative against Transnational Organized Crime. Accessed Dec 31, 2021. https://globalinitiative.net/analysis/un-cybercrime-debate/

Walker, Summer. “Cyber-insecurities? A guide to the UN cybercrime debate.” Global Initiative against Transnational Organized Crime. Accessed Jan 10, 2022. https://globalinitiative.net/analysis/un-cybercrime/

Wang, Yuxin. “Design and Implementation of Multi-interface Virtual Real-time Operating System on Windows Platform.” Accessed Feb 9, 2022. https://xueshu.baidu.com/usercenter/paper/show?paperid=1x6q0tv0w42e0c10646e0am0w0416991.

Waters, Richard and Patti Waldmeir. “Yahoo Loses Nazi Memorabilia Case.” Financial Times. Jan 15. 2022 accessed. https://www.ft.com/content/81127f12-83cb-11da-9017-0000779e2340.

Wei, Pei. "On the Enforcement Jurisdiction in Cross-Border Data Investigation against Cybercrime." Journal of Comparative Law, no. 6 (2021).

Whal-Jorgensen, Karin. “Is WikiLeaks Challenging the Paradigm of Journalism? Boundary Work and Beyond.” International Journal of Communication, vol.8(2014): 1-12.

Yi, Ming. “EU Cracks down on ‘Dark Web’ Drug Sellers, Seizing 5.2 Million Dollars in Cryptocurrency.” BiaNews. Feb 27, 2022 accessed. http://www.bianews.com/news/details?id=15295&type=0.

Zhu, Bonnie, Anthony Joseph and Shankar Sastry. "A Taxonomy of Cyber Attacks on SCADA Systems.” 2011 International, Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 380-388.

Ziolkowski, Katharina. “General Principles of International Law as Applicable in Cyberspace." In Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, ed. Katharina Ziolkowski, 135-88. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013.

Ziolkowski, Katharina. "Peacetime Cyber Espionage-New Tendencies in Public International Law." In Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, edited by Katharina Ziolkowski, 425-64. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2013.