SOI
2024

GUIA ACESSÍVEL

United Nations Office on Drugs and Crime - UNODC

UNIÃO NORTE-RIOGRANDENSE DOS ESTUDANTES DE DIREITO INTERNACIONAL

SIMULAÇÃO DE ORGANIZAÇÕES INTERNACIONAIS

UNITED NATIONS OFFICE ON DRUGS AND CRIME

PROFESSOR COORDENADOR: Diogo Pignataro de Oliveira

PROFESSOR COORDENADOR-ADJUNTO: Thiago Oliveira Moreira

DIRETORIA DA UNEDI

- **Secretário-Geral**: José Carlos Sobrinho Neto
- **Vice-Secretária-Geral**: Juliana Anita Macêdo Pereira de Paula
- **Primeira-Secretária:** Pamela Araújo Xavier de Paiva
- **Segunda-Secretária**: Maria Antônia de Souza Ferreira
- **Primeira-Tesoureira:** Renata Briolanja Araujo Xavier
- **Segunda-Tesoureira**: Ana Isabel Fernandes Sousa

DIRETORIA DA UNODC

- **Diretoras Acadêmicas:** Maria Eduarda de Melo Silva Nogueira e Raissa Villar Rodrigues
- **Diretores Assistentes:** Arthur Gabriel Pereira Espínola, Augusto Etrusco Itabaiana, Cecília Nunes de Carvalho, Evelyn Emily Vasconcelos Lopes, Luiza Carla de Medeiros Bezerra e Rafael Pinheiro Camelo
- **Tutor:** Yuri Luis Pinheiro Morais Goes

23° Edição

Natal, Rio Grande do Norte, 2024

ABSTRACT

This study's main intent is to provide an initial assisting perspective to participating delegates of the 23rd Edition of the Simulation of International Organizations (SOI) by giving perspective on what topics the United Nations Office on Drugs and Crime (UNODC) agenda consists of. The present compilation brings a reflective outlook on modern day societal problems involving technology, industries digitization processes and how Public and Private entities are affected by those on broader scales than ever before. Firstly, the participation of Member States and cooperative stakeholders Observers in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is highlighted, followed by an overview on the implementation processes of measures adopted by them. In order to achieve reliable results a foundation was created off of official documents, trusted journalistic literature and public representative statements. Lastly, a provisioning scenario regarding Research and Development of new generation technologies and the sprouting presence of Artificial Intelligence worldwide was revised regarding delegation's official projects, indicating a whirlwind future when daily commuting action tools are affected by inevitable, lucrative platforms.

Keywords: UNODC, Cybercrime, Cybersecurity, R&D, Artificial Intelligence.

ABBREVIATIONS LIST

AFIS – Automated Fingerprint Identification System

AI – Artificial Intelligence

ANPD – **Autoridade Nacional de Proteção de Dados**

ANS – **Agência Nacional de Saúde**

ANUIES – National Association of Universities and Institutions of Higher Education

ARPANET – Advanced Research Projects Agency Network

ASEAN – Association of Southeast Asian Nations

ASN – Autonomous System Number

C2S – Client to server encryption

CAC – Cyberspace Administration of China

CCDCoE – Cooperative Cyber Defence Center of Excellence

CCF– Commission for the Control of INTERPOL's Files

CCOC – Joint Cyber Command

CCP – Container Control Programme

CCP – Chinese Communist Party

CCP – Cyber Police Center

CEO – Chief Executive Officer

CERTs – Central Emergency Response Teams

CFAA – The Computer Fraud and Abuse Act

CFI – Leverhulme Centre for the Future of Intelligence

CIIP – Critical Information Infrastructure Protection Department

CISA – Cybersecurity and Infrastructure Security Agency

CMA – Computer Misuse Act 1990

CNCiber **– Comitê Nacional de Cibersegurança**

ColCERT – Colombian Cyber Emergency Response Group

CPR – Check Point Research

CRASSH – Centre for Research in the Arts, Sciences and Humanities

CSER – Centre for the Study of Existential Risk

CSIRT – Computer Security Incident Response Team.

CSL – Cybersecurity Law

CTED – United Nations Counter-Terrorism Committee Executive Directorate

DDoS – Distributed Denial-of-Service

DFG – **Deutsche Forschungsgemeinschaft**

DHS – Department of Homeland Security

DoD – United States Department of Defense

DORA – Digital Operational Resilience Act

DSIT – Department for Science, Innovation and Technology

DSL – Data Security Law

E2E – End-to-end encryption

ECL – Electronic Commerce Law

ECTA – Electronic Communication and Transactions Act 25 of 2002

ENISA – European Union Agency for Cybersecurity

EU – European Union

EV – Electric Vehicle

FBI – Federal Bureau of Investigation

FFRDC – Federally Funded Research and Development Center

FHI – Future of Humanity Institute

FPA – Films and Publications Act

FSB – Russian Federal Security Service

FTC – Federal Trade Commission

FTCA – Federal Trade Commission Act

FTF– Foreign Terrorist Fighters

GCC – Google Cloud Console

GDP – Gross Domestic Product

GDPR – General Data Protection Regulation

GERD – Gross Domestic Expenditure on Research and Development

GII – Global Innovation Index

GI-TOC – Global Initiative Against Transnational Organized Crime

GLB – Gramm-Leach-Bliley Act

GLOTIP – Global Report on Trafficking in Persons

GReAT – Kaspersky Lab's Global Research and Analysis Team

GSA – United States' General Services Administration

GSAIS – Graduate School of Advanced Integrated Studies in Human Survivability

HOTP – HMAC-based One-Time Password

ICCS – International Classification of Crime for Statistical Purposes

ICS – Industrial Control Systems

ICT – Information and Communication Technology

ICTA – Information Technologies and Communications Authority

IDC – International Data Corporation

IHL – International Humanitarian law

IMEI – International Mobile Equipment Identity

IMF – International Monetary Fund

IMSI – International Mobile Subscriber Identity

INL – Idaho National Laboratory

INTERPOL – International Criminal Police Organization

IoT – Internet of Things

IPC – Indian Penal Code

IPO – Initial Public Offering

IROs – Independent Research Organizations

ISWAP – Islamic State West Africa Province

IT – Information Technology

ITH – Institute for Technology and Humanity

ITU – International Telecommunication Union

KKL – Estonian Defense League’s Cyber Unit

LGPD – **Lei Geral de Proteção de Dados**

LLM – Large Language Models

MCMP – Munich Centre for Mathematical Philosophy

MIT – Massachusetts Institute of Technology

ML – Machine Learning

MSJE – Ministry of Social Justice and Empowerment

MVD – Ministry of Internal Affairs

NACTA – National Counter Terrorism Authority

NASA – National Aeronautics and Space Administration

NATO – North Atlantic Treaty Organization

NCA – National Crime Agency

NCA – National Cybersecurity Authority

NCSC – National Cyber Security Centre

NCST – Nigerian Council for Science and Technology

NIS2 – Network and Information Security Directive

NITDA – National Information Technology Agency

NRM – National Referral Mechanism

NSA – National Security Agency

OCG – Organizations Crime Groups

OCINDEX – Global Organized Crime Index

OECD – Organization for Economic Co-operation and Development

PCUs – Port Control Units

PDPL – Personal Data Protection Law

PIPL – Personal Information Protection Law

PNCiber – **Política Nacional de Cibersegurança**

PRC – People’s Republic of China

PUBG – PlayerUnknown's Battlegrounds

R&D – Research and Development

RDT&E – Research, Development, Test And Evaluation

RENASEC – National Computer Security Network

RIA – Estonian Information Systems Authority

ROCUs – Regional Organized Crime Units

RSA – Republic of South Africa

RTOs – Research and Technologies Organizations

S&T – United States Science and Technology Directorate

SLTT – State, Local, Tribal and Territorial Governments

SMEs – Small and Medium-Sized Enterprises

SOE – State-owned enterprise

SSU – Security Service of Ukraine

TAO – Tailored Access Operations Unit

TOTP – Time-based OneTime Password

TSE – ***Tribunal Superior Eleitoral***

UK – United Kingdom of Great Britain and Northern Ireland

UKRI – United Kingdom Research and Innovation

UN – United Nations

UNCAC – United Nations Convention Against Corruption

UNCT – United Nations Country Team

UNOCT – United Nations Office of Counter-Terrorism

UNODC – United Nations Office on Drugs and Crime

UNPDTF – United Nations Peace and Development Trust Fund

UNTOC – UN Convention on Transnational Organized Crime

USA – United States of America

USPS – United States Postal Service

USSR – Union of Soviet Socialist Republics

WCI – World Cybercrime Index

WCO – World Customs Organization

WWW – World Wide Web

SUMMARY

1 INTRODUCTION

The United Nations Office on Drugs and Crime (UNODC) is an international entity created to support the creation and maintenance of regulations, as well as the cooperation between countries and organizations in combating the spread of transnational organized crime. Through its work, it aims to help nations translate international treaties into national laws, and thus provide a safer environment to all people.

The purpose of this committee at SOI XXIII is to simulate a session of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. More specifically, it aims to tackle the subjects of the “Criminal Usage of Cyber-space: Illicit online trading and malicious R&D of new technologies”.

This Annex Guide will provide supportive information about the participating members in the committee, serving as a substantial base to further studies on the matter. These delegations include countries, companies, institutes and interested parties that can further provide help to the development of a resolution document. Hence, all positions presented in this document were based on available information, not solely reflecting the position of a delegation, but an overall view of its activities and history in the cybersphere.

In brief, this guide will serve as a starting point from where the delegates will deepen their studies on the subjects to be discussed during the simulation. The delegates are, then, further encouraged to research independently, gathering all the remaining information they may find relevant and that may not be included in the present text, thus

preparing themselves and expanding their knowledge beyond what is given.

2 AFRICA:

The African continent as a whole is rapidly expanding in accessibility to the internet, with a user base of 570 million as of 2022, doubling its total in less than a decade.[1] To support this growing phenomenon and to guarantee that people will have a safe, private, and overall positive experience on-line, countries have administered domestic laws and regulations, while also working together to try and safeguard African cyberspace.[2]

However, the research and development (R&D) of new technologies in the world's poorest continent doesn't grow akin to its internet access. According to the World Bank, African countries spend less than the world average in R&D, scoring a medium expenditure of 0.45% of their GDP on it. Thus, to grant their people a better shot at a more equal society and economic development, it is necessary to start tackling the issue at hand.[3]

2.1 FEDERAL REPUBLIC OF NIGERIA

[1]GALAL, Saifaddin. **Internet usage in Africa - statistics & facts.** Statista, January 19, 2024. Available at: https://www.statista.com/topics/9813/internet-usage-in-africa/#:~:text=The%20continent%20had%20around%20570,41%20million%20in%20South%20Africa. Accessed on: May 31, 2024.

[2]AFRICAN UNION. **African Union Convention on Cyber Security and Personal Data Protection.** Malabo, 2014. Available at: fromhttps://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Accessed on: May 20, 2024.

[3]WORLD ECONOMIC FORUM. **Innovative approaches for unlocking R&D funding in Africa.** November 9, 2023. Available at: https://www.weforum.org/agenda/2023/11/innovative-approaches-for-unlocking-research-and-development-funding-in-africa/. Accessed on: May 31, 2024.

The Federal Republic of Nigeria, a country situated in West Africa, it is the sixth most populous country in the world and the most populous African country, with a population of roughly 228,6 million people in 2024.[4] Nigeria has been a signatory of the United Nations Office on Drugs and Crime (UNODC) since December 9, 2003, becoming a ratified member on December 14, 2004.[52]

Nigeria made its first effort towards Research and Development (R&D) in 1970, establishing the Nigerian Council for Science and Technology (NCST), with its modern equivalent being the Ministry of Science and Technology.[6] In April 2001, the National Information Technology Agency (NITDA) was created to implement the Nigerian Information Technology Policy and coordinate the country's IT development.[7]

The National Information Technology Development Act (2007) delimitates the creation of a framework for the several steps involved in R&D, those being the planning, development, standardization, application, coordination, monitoring, evaluation, and regulation of Information Technology (IT) activities, practices, and systems in Nigeria.[8]

Developing, regulating, and advising on IT in the country, the NITDA is the most important Agency for e-government implementation,

---

[4]WORLDOMETER. **Nigeria Population (2024).** Available at: https://www.worldometers.info/world-population/nigeria-population/. Accessed on: May 23, 2024.

[5]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles.** Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Fnga.html. Accessed on: May 23, 2024.

[6]NATIONAL BUREAU OF STATISTICS. **Research and Development Statistics.** Available at: https://www.nigerianstat.gov.ng/pdfuploads/RESEARCH%20AND%20DEVELOPMENT.pdf. Accessed on: May 23, 2024.

[7]NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA). **Research and Development Department.** Available at: https://nitda.gov.ng/background/. Accessed on: May 23, 2024.

[8]NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **National Information Technology Development Agency Act 2007.** Available at: https://nitda.gov.ng/wp-content/uploads/2020/11/NITDA-ACT-2007-2019-Edition1.pdf. Accessed on: May 23, 2024.

Internet governance and general IT development in Nigeria. Its objectives are the improvement of the strategic alignment and coordination of indigenous IT research efforts with global industry requirements, and promote technology tracking, acquisition, adoption and adaptation for a sustainable digital economy.[9]

One of the NITDA's special purpose vehicles, the National Centre for Artificial Intelligence and Robotics (NCAIR) promotes research and development on emerging technologies and their practical applications. As a research facility, some of NCAIR focuses are Artificial Intelligence (AI), Robotics and Drones, Internet of Things (IoT), job creation, National development, and creating a thriving ecosystem for innovation-driven entrepreneurship (IDE).[10]

On June 2012, the Ministry of Communication Technology released the National Information and Communication Technology (ICT) Policy, with the main objective of creating a conducive environment for the rapidly expansive ICT networks and services, with some specific objectives facilitating the development of an appropriate legal framework for effective implementation of ICT policies, and unification of all Policy Administrators under a single Ministry.[11]

Furthermore, in addition to being a party member to the Budapest Convention on Cybercrime, in February 2015, the Nigerian Government released the National Cybersecurity Policy and Strategy, which is the acting legislation on cybercrime in the country. Based on the

---

[9]NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **Research and Development Department.** Available at: https://nitda.gov.ng/department/research-and-development-department/. Accessed on: May 23, 2024.

[10]NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **National Center For Artificial Intelligence and Robotics.** Available at: https://nitda.gov.ng/ncair/. Accessed on: May 23, 2024

[11]THE MINISTRY OF COMMUNICATION TECHNOLOGY. **National Information and Communication Technology (ICT) Policy.** Available at: https://nitda.gov.ng/wp-content/uploads/2020/06/National-ICT-Policy1.pdf. Accessed on: May 24, 2024.

understanding that threats to information and communication technology are matters of National security, the most significant threats regulated are cybercrime, cyber-espionage, cyber conflict, cyber-terrorism and child online abuse and exploitation.[12]

Regarding the trafficking activity in the country, according to the 2023 Global Organized Crime Index (OCINDEX) made by the Global Initiative Against Transnational Organized Crime (GI-TOC), Nigeria's highest trafficking markets are arms trafficking and synthetic drug trade. A significant security's concern, Nigeria is a transit and destination country for illicit weapons, a trade market that is driven by forces like armed violence, banditry, and conflict with violent extremist groups. The insecurity leads local communities and vigilantes to acquire arms for self-defense. The market is fed by both international and local artisanal gun manufacturers.[13]

On the illegal drugs market, Nigeria has an important role in the synthetic drugs trade, and is a major transit point in heroin trade, with the country also presenting a high level of heroin use, which could be associated with easy access, poverty, job insecurity and unemployment. With a prevalent cultivation of Cannabis in the country, Nigeria serves as a significant spot on its market, being a departure, transit, and destination point.[14]

Moreover, another prevalent issue is human trafficking, with networks operating in, most notably, sex trafficking and labor exploitation. There also are Nigerian networks illegally smuggling people

---

[12]COUNCIL OF EUROPE. **Cybercrime policies/strategies.** Available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/nigeria/pop_up. Accessed May 24, 2024.

[13]THE ORGANIZED CRIME INDEX. **Nigeria.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_nigeria_2023.pdf. Accessed on: May 24, 2024.

[14]*Ibidem.*

towards primarily European countries, mostly due to levels of poverty and population size. Kidnappings driven by ransom and extortion, and protection racketeering pose major challenges for Nigerian security, with kidnappings evolving from non-violent transactional crimes to lethal violence.[15]

The targeting and extortion of LGBTQ+ individuals through dating apps have increased since the implementation of an anti-LGBTQ+ law in January 2014, highlighting the cybersecurity question in the country. The quasi-governance of extremist group Islamic State West Africa Province (ISWAP) in the North of Nigeria has become an example of protection racketeering, though the dynamics are still extremely violent.[16]

The cybercrime threat has increased in Nigeria, though cybercrimes targeting individuals are less common than those attacking major organizational systems, national security, and critical infrastructure databases. Furthermore, Environmental crimes are leading to the destruction of the local fauna and flora, with cases such as wildlife trafficking, especially pangolin scales and ivory, and timber exploitation.[17]

Since 2013, during the violence outbreak in the north of Nigeria and the emergence of Boko Haram as a serious threat to regional stability, UNODC has worked together with the Government of Nigeria, the European Union (EU) and the United Nations Counter-Terrorism Committee Executive Directorate (CTED) with the purpose of strengthening the capacity of Nigerian criminal justice officials to

[15]THE ORGANIZED CRIME INDEX. **Nigeria.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_nigeria_2023.pdf. Accessed on: May 24, 2024.
[16]THE ORGANIZED CRIME INDEX. **Nigeria.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_nigeria_2023.pdf. Accessed on: May 24, 2024.
[17]*Ibidem.*

effectively investigate, prosecute and adjudicate terrorism cases, following the rule of law, human rights and international best practice.[18]

Subsequently, Nigeria and UNODC would increase the country's criminal justice capability by also focusing on the recent rise of cybercrime, with such collaboration strengthening the combat against cybersecurity threats.[19]

2.2 REPUBLIC OF SOUTH AFRICA

The southernmost country on the African continent, the Republic of South Africa (RSA) has been a part of the United Nations since its conception in 1945,[20] and has significantly aided UN's actions in fighting the widespread of international organized crime throughout the years. It is a signatory of the Single Convention on Narcotic Drugs (1961)[21] and the Convention against Transnational Organized Crime (2000)[22], both of those under the guard of the United Nations Office on Drugs and Crime.

As transnational organizations and lone criminals turned to the internet as both a means and enabler for their illegal activities, the RSA had to evolve and adapt to restrain their operations. Also, with an

[18]UNITED NATIONS. **EU–Nigeria–UNODC–CTED Partnership Project to Counter Terrorism and Violent Extremism Closes.** Available at: https://www.unodc.org/conig/en/eunigeriaunodccted-partnership-project-to-counter-terrorism-and-violent-extremism-closes.html. Accessed on: May 24, 2024.
[19]*Ibidem.*
[20]UNITED NATIONS. **Member States.** Available at: https://www.un.org/en/about-us/member-states#gotoS:~:text=20%2D09%2D1960-,South%20Africa,-Date%20of%20Admission. Accessed on: May 19, 2024.
[21]UNITED NATIONS.**15. Single Convention on Narcotic Drugs, 1961.** New York, 1961. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-15&chapter=6. Accessed on: May 20, 2024.
[22]UNITED NATIONS. **12. United Nations Convention against Transnational Organized Crime**. New York, 2000. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en. Accessed on: May 20, 2024.

estimate of around 45.3 million users as of January 2024[23] — reflecting a growth of over 900% throughout the 2010s and into the 2020s[24] — more and more South Africans have become targets for those transgressors, who often seek to acquire their private data for profit or exploit them as potential clients to illicit e-commerce.

Thus, in May 2021, the African nation signed the Cybercrimes Act 19 of 2020, establishing a plethora of new offenses related to the internet, computers and data, amongst them, hacking and interception of data.[25] Moreover, other laws can be indirectly adopted to subsidize the combat of cyber violations, namely, the Electronic Communication and Transactions Act 25 of 2002 (ECTA), and the Films and Publications Act (FPA), both with capacities to regulate online child pornography, for example.[26]

Internationally, alongside the aforementioned conventions, South Africa is a signatory of both the Budapest Convention on Cyber Crime and the African Union Convention on Cyber Security and Protection of Personal Data (Malabo Convention). However, neither are ratified as of May 2024.[27/28] Ratifying these conventions is paramount, not only to

---

[23]GALAL, Saifaddin. **Number of internet users in Africa as of January 2024, by country (in millions).** Statista, 2024. Available at: https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/. Accessed on: May 19, 2024.

[24]**SA INTERNET growth accelerates.** South Africa. World Wide Worx, 2010. Available at: https://www.worldwideworx.com/sa-internet-growth-accelerates/. Accessed on: May 20, 2024.

[25]REPUBLIC OF SOUTH AFRICA. **Act No. 19 of 2020: Cybercrimes Act, 2020.** Cape Town: Government Gazette, 1 June 2021. Available at: https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf. Accessed on: May 19, 2024.

[26]MTHEMBU, Mpakwana Annastacia. High road in regulating online child pornography in South Africa. *In:* **Computer Law & Security Review.** South Africa: Elsevier Ltd, 2012. Vol. 28, 4 ed, 438-444. Available at: https://doi.org/10.1016/j.clsr.2012.05.010. Accessed on: May 19, 2024.

[27]COUNCIL OF EUROPE. **The Budapest Convention (ETS No. 185) and its Protocols.** Budapest, 2001. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed on: May 20, 2024.

[28]AFRICAN UNION. **African Union Convention on Cyber Security and Personal Data Protection.** Malabo, 2014. Available at: fromhttps://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Accessed on: May 20, 2024.

enhance international cooperation in combating cybercrimes, but to harmonize domestic regulations among member nations.[29]

Nevertheless, all those efforts seem unable to stop the growth in cyber felonies, as South Africa ranked 5th globally in cybercrime density in 2022.[30] One of RSA's most emblematic web related infractions is the illegal trade of wildlife, in particular, the rhino horn trade that led to the killings of 4,500 rhinos between 2011 and 2015 to supply the Asian demand.[31] The purchase of counterfeit goods and piracy has also risen online, with statistics claiming about 30% of consumers admitted to unknowingly buying fake goods when making online purchases.[32]

As the internet continues to evolve, the Rainbow Nation, as it is palso remarked, is investing in its future by developing and researching new technologies to improve both online and offline life. In the 2021-22 period, the gross domestic expenditure on research and development (GERD) as a percentage of the Gross Domestic Product (GDP) went from 0.60% to 0.62%, a growth of 6.9%.[33]

Furthermore, targeting to spend 1.5% of its GDP in R&D, the South African government is the biggest funder in the sector, as enterprises don't seem too keen on giving much attention to this task.[34] It

---

[29]MTUZE, Sizwe Snail ka. MUSONI, Melody. **An overview of cybercrime law in South Africa**. International Cybersecurity Law Review, 2023. Vol 4, 299–323. Available at: https://doi.org/10.1365/s43439-023-00089-8. Accessed on: May 20, 2024.

[30]SURFSHARK. **Cybercrime statistics.** 2022. Available at: https://surfshark.com/research/data-breach-impact/statistics. Accessed on: May 20, 2024.

[31]SHELLEY, Louise I. **Dark commerce: how a new illicit economy is threatening our future.** Princeton: Princeton University Press, 2018.

[32]INTERPOL. **Online African organized crime from surface to dark web.** 2020. Available at: https://enactafrica.org/research/interpol-reports/online-african-organised-crime-from-surface-to-darkweb. Accessed on: May 20, 2024.

[33]REPUBLIC OF SOUTH AFRICA. **SA records an increase in research and development expenditure after COVID-19.** South Africa: South African Government News Agency, January 2024. Available at: https://www.sanews.gov.za/south-africa/sa-records-increase-research-and-development-expenditure-after-covid-19. Accessed on: May 20, 2024.

[34]REPUBLIC OF SOUTH AFRICA. **Survey shows that high proportion of R&D funding comes from government.** South Africa: South African Government News Agency, 2023. Available at:

is difficult to find data on South African companies with R&D programs, as experts cry for more investments in the sector.[35]

As observed, although significant growth is still needed, the Republic of South Africa has clearly been working to improve its laws and investments in the technology sector despite the challenges such endeavors provide. The nation seems to be leaning in the right direction towards reaching its goals, with its ambitions leading the way to further development.[36]

https://www.dst.gov.za/index.php/media-room/latest-news/3857-survey-shows-that-high-proportion-of-r-d-funding-comes-from-government. Accessed on: May 20, 2024.

[35]NICHOLSON, Craig. **R&D in Africa: 'We need to invest more'.** Durban: Research Professional News, June 2023. Available at: https://www.researchprofessionalnews.com/rr-news-world-2023-6-r-d-in-africa-we-need-to-invest-more/. Accessed on: May 20, 2024.

[36]*Ibidem.*

3 AMERICA

America's colonization history constituted by culturally rich but economically impoverished countries draws a straight line for understanding how the continent has been a pop-culture reference for narcotrafficking, crime fighting operations and since such problems have changed reality platforms, cybercrime has installed itself as a new impending phenomenon.[37]

As a territory that serves as an umbrella to so many majorly acting countries, it has shown great growth and technology based on positive transformation scoring. Nations' Research & Development actions budgets have adapted alongside admirable legal frameworks which show increased potential for establishing global cybersecurity leadership missions as far as international cooperation amongst members follows.[38]

3.1 FEDERATIVE REPUBLIC OF BRAZIL

The Federative Republic of Brazil has played various remarkable diplomatic roles in partnership with UNODC.[39] Having participated in human and drug trafficking, corruption fighting and money laundering conventions, those include full engagement in reaching consensus for minimal standardization of criminalization concepts, normative enabling for timely investigation and prosecution, international legal cooperation and electronic data preservation and monitoring in the convention on

[37]INTERPOL. **Cybercrime Capacity Building in the Americas.** Available at: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cybercrime-Capacity-Building-in-the-Americas. Accessed on: May 31, 2024.
[38]*Ibidem.*
[39]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **About the Liaison and Partnership Office in Brazil.** Available at: https://www.unodc.org/lpo-brazil/en/sobre-unodc/index.html. Accessed on: May 21, 2024.

countering the use of information and communications technologies for criminal purposes.[40]

The country has been appointed by various tech enterprises as the second most vulnerable place for cyber attacks, with over 1,500 system storming attempts per minute.[41] Additionally, the country ranks number one when it comes to financial scams as piracy and unsolicited adware flood, an intensified post pandemic scenario where retail, agribusiness and education are at risk.[42]

Regular online banking use, digital only accounts, and quick adoption of fintechs by citizens are also contributing factors. Pix, an instant-payment platform was introduced and around 3bn transactions a month have helped the 1.8m banking trojans mark within a year,[43] a change for the decade long money mules tactic, both reported by Kaspersky Lab.[44]

Additionally, threats have affected health assistance, technology, and energy governmental sectors the most. Patient's data are targeted through ransomware invasions. Enterprises have not set ground for precaution while the State struggles to maintain confidentiality.[45]

---

[40]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Brazilian Government's position regarding the objectives, scope and structure of an international convention on countering the use of information and communications technologies for criminal purposes.** Available at: :h ttps://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Brazil_AHC_Brazilian_Position.pdf. Accessed on: May 21, 2024.

[41]MARI, ANGELICA. **Brazil Is The World's Second Most Vulnerable Country To Cyberattacks.** Available at: https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/?sh=7849be9b27a4. Accessed on: May 21, 2024.

[42]THE NATIONAL. **Cybercrime in Brazil.** Available at: https://youtu.be/X67-UTAyols?si=Kib4yXlZ2TJeUOBg. Accessed on: May 21, 2024.

[43]THE ECONOMIST. **Why is Brazil a hotspot for financial crime?.** Available at: https://www.economist.com/the-americas/2024/01/04/why-is-brazil-a-hotspot-for-financial-crime. Accessed on: May 21, 2024.

[44]KASPERSKY. **Brazil Banks in the Malware Glare**. Available at: https://www.YouTube.com/watch?v=3h-vUWFRsLs. Accessed on: May 21, 2024.

[45]CLARANET. **Cibersegurança: veja os setores mais críticos no Brasil.** Available at: https://www.claranet.com/br/blog/ciberseguranca-veja-os-setores-mais-criticos-no-brasil. Accessed on: May 21, 2024.

Brazil's large territory imposes a harder time with traditional cooperative mechanisms and due to it, prioritizing prevention and enhancing knowledge on cybersecurity has shown itself to be as important as tackling criminal cases.[46] With that in mind, two national-level Computer Emergency Response Teams (CERTs), CTIR.gov and CERT.br., were arranged for crisis management and national legislation made to be a priority.[47]

The right to privacy is deemed by the civil code as a personality right and Brazil has a wide range of federal and state laws on criminal volatility of technological devices correspondence, warranties, and duties for the protection of logs and private communication such as the Internet Legal Framework (**Marco Civil da Internet**).[48/49]

In addition, influenced by the European General Data Protection Regulation (GDPR), 2018's General Data Protection Law (**Lei Geral de Proteção de Dados** - LGPD) unifies 40 different laws on the processing of personal data creating the Brazilian Data Protection Authority (**Autoridade**

Nacional de Proteção de Dados - ANPD) which tests cooperation between private and public sectors watching for the

[46]*Ibidem.*

[47]GLOBAL CYBER SECURITY CAPACITY CENTER. **Cyber Security Capacity Review.** Available at: https://www.gov.br/gsi/pt-br/ssic/eventos/CMMreportBrazil2023_finalversoemingls.pdf. Accessed on: May 21, 2024.

[48]*BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018.*** Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: May 21, 2024.

[49]INHOUSELAWYER. **Data protection and cybersecurity in Brazil.** Available at: tituhttps://www.inhouselawyer.co.uk/legal-briefing/data-protection-and-cybersecurity-in-brazil/. Accessed on: May 21, 2024.

furthering of international data, notifying authorities and economically punishing wrongdoers.[50]

Fake news has been a reason for chaotic interactions in Brazil long before concerned measures were taken. The 2018's federal elections were directly affected by the misinformation on candidates and 2022's were at least pivoted because of the doubtful broadcasts on the system itself.[51] To discern future dangers the Superior Electoral Court (**Tribunal Superior Eleitoral - TSE**) has stormproofed it since 2009 and reported attempting criminals so that cyberattacks or the reporting of votes would not be promptly affected any further.[52]

A bill on AI inspired by the Organization for Economic Co-operation and Development (OECD) was drafted in 2020 but damage, inaccuracy and risks of artificial intelligence were not addressed.[53] Fast forward to 2024, as preventive electoral regulations, the use of false imitation content, mediating chat boxes and avatars were prohibited, and other digital creative tools of the same matter were placed under labeling obligation and approval as non-harmful media.[54]

In December 2023, a presidential decree instituted the National Cyber Security Policy (Política Nacional de Cibersegurança - **PNCiber**)[55]

---

[50]BAKERMCKENZIE. **Global Data Privacy and Cybersecurity Handbook.** Available at: https://resourcehub.bakermckenzie.com/pl-pl/resources/global-data-privacy-and-cybersecurity-handbook/latin-america/brazil/topics/key-data-privacy-and-cybersecurity-laws. Accessed on: May 21, 2024.

[51]CONTEXT. **Brazil election: Platforms are not curbing disinformation.** Available at: https://www.context.news/surveillance/opinion/brazil-election-platforms-are-not-curbing-disinformation. Accessed on: May 21, 2024.

[52]MUGGAH, ROBERT. **Bolsonaro Is Already Undermining Brazil's Upcoming Election.** Available at: https://foreignpolicy.com/2022/05/04/bolsonaro-brazil-election-2022-disinformation-misinformation-digital-social-media/. Accessed on: May 21, 2024.

[53]EUROPEAN UNION. **Promoting irresponsible AI: lessons from a Brazilian bill.** Available at: https://eu.boell.org/en/2022/02/14/promoting-irresponsible-ai-lessons-brazilian-bill. Accessed on: May 21, 2024.

[54]FOLHA DE SÃO PAULO. **Brazilian Electoral Court Regulates Artificial Intelligence in Elections and Prohibits Deepfake Use by Campaigns.** Available at: https://www1.folha.uol.com.br/internacional/en/brazil/2024/02/brazilian-electoral-court-regulates-artificial-intelligence-in-elections-and-prohibits-deepfake-use-by-campaigns.shtml. Accessed on: May 21, 2024.

[55]*BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Diário Oficial da União. Brasil, ano 23, n. 245, 1, p. 10. 26 dezembro***

and the National Cybersecurity Committee (**Comitê Nacional de Cibersegurança - CNCiber)**.[56] Intentions with both promoting national products and services, educational measures, fighting malicious activity and improving not only safety standards but junctions of republican powers branches.[57]

Great advantage from a safer environment is highlighted by the use of Artificial Intelligence. Numbers prove the largest country in Latin America to also be the biggest usual consumer, 15% more interested in AI tools than the rest of the globe,[58] and expects that it will add up by 4.2% to the national Gross Domestic Product (GDP) by the year 2030.[59/60] Forwarding governmental missions on a different note, Artificial Intelligence projects are being made useful for national worldwide educational source funding through federal universities and the Ministry of Science, Technology and Innovation research investing page.[61]

Furthermore, tackling threatening remarks to the functioning of the health system the National Health Agency **(Agência Nacional de Saúde - ANS**) has joined the public Digital Transformation Plan strategy and is looking to amplify workarounds for health insurance beneficiaries,

---

2023. Available at: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Accessed on: May 21, 2024.

[56]GOV.BR. ***Comitê Nacional de Cibersegurança.*** Available at: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber. Accessed on: May 21, 2024.

[57]MATTOS FILHO. **Decree establishing Brazil's National Cybersecurity Policy enacted**. Available at: https://www.mattosfilho.com.br/en/unico/brazils-cybersecurity-policy/. Accessed on: May 21, 2021.

[58]MARI, ANGELICA.**Brazil Among Most Optimistic Countries About AI, Study Says.** Available at: https://www.forbes.com/sites/angelicamarideoliveira/2023/11/03/brazil-among-most-optimistic-countries-about-ai-study-says/?sh=63edc4572daa. Accessed on: May 21, 2024.

[59]PAGBRASIL. **The State of Generative AI in Brazil.** Available at: https://www.pagbrasil.com/insights/generative-ai/#:~:text=Brazil%2C%20as%20the%20most%20enthusiastic,uses%20generative%20AI%20with%20Microsoft. Accessed on: May 21, 2024.

[60]PACETE, LUIZ GUSTAVO. ***Por que 2023 será o ano da inteligência artificial?***. Available at: https://forbes.com.br/forbes-tech/2023/01/por-que-2023-sera-o-ano-da-inteligencia-artificial/. Accessed on: May 21, 2024.

[61]GOV.BR. **Brazil will use data science and A.I. to bring together investments in science and technology projects.** Available at: https://www.gov.br/en/government-of-brazil/latest-news/2022/brazil-will-use-data-science-and-a-i-to-bring-together-investments-in-science-and-technology-projects. Accessed on: May 21, 2024.

companies' data registration, operators overseeing and quicken the public health system reimbursement actions, bringing citizens liability options.[62]

3.2 REPUBLIC OF COLOMBIA

Officially called the Republic of Colombia, this country occupies a strategic location, serving as a bridge between the American continents. It is also the second most populous nation in South America and one of the few – along with Chile – to be part of the Organization for Economic Co-operation and Development (OECD). In this scenario, given its cultural and economic connections, as well as its significant territorial position, Colombia is a key player in Latin America, especially in discussions related to security matters.

Despite being notorious for its vibrant cultural and touristic offerings, such as its dances, diverse foods, and music – particularly, of course, those popularized by Shakira – the country is also internationally known for the presence of drug cartels – within this context the name that stands out is Pablo Escobar. Against a backdrop of social inequality and structural insecurity, Colombia wrestles with internal political conflicts and numerous criminal groups, cementing its status as a global hub for cocaine trafficking.[63]

Given this, the internet and digital means of communication emerge as modern instruments for the international black market.

---

[62]MATTOS FILHO. **Artificial intelligence in Brazilian health and supplementary health services.** Available at: https://www.mattosfilho.com.br/en/unico/artificial-intelligence-health-services/. Accessed on: May 21, 2024.
[63]FRASSON-QUENOZ, Florent; GONZÁLEZ, César Augusto Niño. Colombia's Cybersecurity Predicament: State making, strategic challenges, and cyberspace. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 42, pp. 494-503.

Modalities of payment and acquisition of illegal Arms are extended due to access to enormous economic resources capable of being invested in the strengthening and expansion of narcotrafficking organizations or their support networks.[64]

Therefore, Colombia stands out as a destination for illicit arms trade, facilitated by technological advancements, which allow connections with international traffickers abroad and maximize transaction negotiations through fund transfers.[65] Additionally, the country serves as a production center for the online distribution of synthetic drugs in Latin America, intricately linked to underground commercial routes, especially extending to the Asian continent.[66]

The internet has also functioned as a malicious medium for the media exposure of Colombian cartels, serving as a form of globally successful platform for narco-fiction and relativization of their illicit activities. In this sense, social media platforms have turned into promotional spaces for the daily operations of drug traffickers, with posts covering every aspect from cultivation and production to drug deliveries and the use of clandestine airports, sharing videos about cartel activities in a casual and unfiltered way.

This impact was also amplified by the *Narcos* series – a Netflix production about the life of Pablo Escobar – which spurred a wave of tourist interest in drug trafficking landmarks, revitalizing the reputation of Medellin, although the influence of the cartel only continues to intensify.

---

[64]DUPUY, Pablo Casas (org.). **Violence, crime, and illegal Arms trafficking in Colombia**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: https://www.unodc.org/pdf/Colombia_Dec06_en.pdf. Accessed on: May 25, 2024.

[65]*Ibidem*.

[66]UNODC OPIOID STRATEGY. **The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf. Accessed on: May 25, 2024.

Such “clean-up” of perspective, which promotes the so-called dark tourism, merely perpetuates a trivialization of violence and narcotrafficking organizations.[67]

In such circumstances, the dynamics of physical insecurity are transferred to the virtual framework. Nonetheless, this hasn’t been the only concern for the country in the digital realm, as the challenges of cyberspace can go beyond these limits due to inherent threats of this inhospitable system.

Colombia became the first country in Latin America to adopt cyber defense and cybersecurity strategies to mitigate the risks that endanger national computer security and data transmission.[68] In 2011, a guideline document for the national cyber defense and cybersecurity policy was introduced to define strategies capable to counter the rise of digital threats.[69] The Intersectoral Commission was established to oversee information traffic management, while the Colombian Cyber Emergency Response Group (ColCERT) was tasked to coordinate protective measures in collaboration with the Cyber Police Center (CCP) and the Joint Cyber Command (CCOC).[70]

---

[67]BEAUVAIS, Camille. **Dark tourism, “Netflix tourism”: stakes and conflicts of actors in Medellin**. (Mega) *Evénements urbains et tourisme: pratiques touristiques et organisation spatiale, vol. 22, 2022*. Available at: https://journals.openedition.org/viatourism/8910?lang=ca. Accessed on: May 25, 2024.

[68]KOBEK, Luisa Parraguez; CALDERA, Erick. **Cyber Security and Habeas Data: The Latin American Response to information Security and Data Protection**. Revista Oasis, no. 24, pp. 109-128, Bogotá, 2016. Available at: https://www.redalyc.org/journal/531/53163716007/html/. Accessed on: May 25, 2024.

[69]COLOMBIA. ***Lineamientos de política para Ciberseguridad y Ciberdefensa***. *Bogotá: Documento Consejo Nacional de Política Económica y Social – Conpes* 3701, 2011. Available at: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf. Accessed on: May 26, 2024.

[70]MÉNDEZ, Júlio César Villanueva. ***La ciberdefensa en Colombia***. Institutional Repository *Universidad Piloto de Colombia, Bogotá*, 2015. Available at: https://repository.unipiloto.edu.co/handle/20.500.12277/2812. Accessed on: May 25, 2024.

Image 01: Colombian cyber defense coordination model

Source: Documento Conpes 3701.[71]

By leveraging this structure, the state set up protection strategies and online privacy standards to defend the integrity of governmental data and information, thereby reinforcing internal institutions and improving their accessibility. Furthermore, Colombia was also one of the pioneering nations worldwide to introduce a regulation specifically targeting cyberspace, through Law n. 1273 that amended new legal rights in the Penal Code.[72]

In conclusion, the country's ongoing challenges with security matters, such as drug cartels, social inequality, or trivialization of violence highlights a multifaceted concern which requires appropriate policy measures. The digital realm further complicates these dynamics, as it facilitates clandestine markets and intensifies illicit activities.

[71]COLOMBIA. ***Lineamientos de política para Ciberseguridad y Ciberdefensa***. *Bogotá: Documento Consejo Nacional de Política Económica y Social* – Conpes 3701, 2011. Available at: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf. Accessed on: May 25, 2024.
[72]FRASSON-QUENOZ, Florent; GONZÁLEZ, César Augusto Niño. Colombia's Cybersecurity Predicament: State making, strategic challenges, and cyberspace. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 42, pp. 494-503.

By being the first Latin American country to adopt cybersecurity strategies and to structure a cyber defense system, Colombia demonstrates a proactive approach to mitigating digital threats. Thus, the country places itself in the position of a regional protagonist in dealing with cyber risks and crimes.

3.3 UNITED MEXICAN STATES

Since 2006, the United Mexican States has hosted an Office on Drugs and Crime with a regional approach. In 2012, this relationship was further strengthened with the establishment of a Liaison and Strategic Partnership Office.[73]

Despite being situated in North America, Mexico is deeply connected to the “Latin American” spirit, sharing cultural interests, economic trends and even security concerns. In turn, the technological advancements and cyber impacts in the country are influenced by its proximity to the United States. This way, the digital realm for Mexico proves to be challenging due to its complexity in social development. The internet’s anonymity and boundless opportunities have facilitated the growth of illegal trade and illicit activities.

Indeed, it reveals itself as a modality of action for narcotrafficking, establishing a network of “darknet” associated marketplaces. In this framework, cyberspace acts as an extension for drug cartels[74], which facilitates the sale of substances such as cocaine, marijuana, and

[73]UNODC *EN MÉXICO. **Quiénes somos***. Vienne: United Nations Office on Drugs and Crime, 2024. Available at: https://www.unodc.org/lpomex/es/UNODC-en-Mexico/quienes-somos.html. Accessed on: May 26, 2024.
[74]Examples of cartel marketplaces are extensive, with the *Cartel de Sinaloa* being the most notable, but there is also a highly active of other criminal organizations, including *Los Urabeños* from Colombia, *Cártel de Jalisco Nueva Generación*, Cartel Darknet Shop, Gulf Cartel Texas, and an unspecified crime market simply known as DW Drugs Cartel.

amphetamine crystal shards, as well as offering clandestine services, including hitman-for-hire operations.[75]

In response to evolving regulatory measures, Organizations Crime Groups (OCG) have turned into the dark web and cryptocurrencies to manage the acquisition and shipment of illicit materials. The production of synthetic drugs, unbound by geographic limitations, has taken advantage of the internet to streamline all phases of trafficking, from acquiring precursors to distributing the final products. With a large operation in Latin America and the Caribbean, Mexico plays a crucial role in this manufacturing network, acting as a critical hub in trafficking routes and online forums.[76]

[75]DARKOWL. **Darknet Cartel Associated Marketplaces**. Denver, USA, 2002. Available at: https://www.darkowl.com/blog-content/darknet-cartel-associated-marketplaces/. Accessed on: May 26, 2024.
[76]UNODC OPIOID STRATEGY. **The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf. Accessed on: May 25, 2024.

Image 02: Example of darknet advertisement, with supplier shipping from Mexico.

Source: UNODC OPIOID Strategy.[77]

Incidents in cyberspace, along with inherent digital vulnerabilities and risks, pose some significant challenges for Mexico due to a lack of institutional structures. Although the Government has not established specific cybersecurity procedures, relevant provisions are included in the Federal Criminal Code, especially concerning financial crime, information security, and cybercrimes such as terrorism, kidnapping, as well as, of course, drug trafficking.[78]

Cyberattacks on the Bank of Mexico's systems in 2018, which resulted in an estimated loss of 300 million pesos, served as a critical

[77]UNODC OPIOID STRATEGY. **The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf. Accessed on: May 25, 2024.

[78]KOBEK, Luisa Parraguez. **The State of Cybersecurity in Mexico: An Overview**. Wilson Center, Washington, DC, 2017. Available at: https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview. Accessed on: May 26, 2024.

juncture for the consolidation of a cybersecurity agenda and revealed the impact of such threats.[79] In fact, it also underscored the complex landscape facing Mexico, intricately linked to its national economic and political conditions, its position as a mid-level player in North American and trans-Pacific trade dynamics, and its role as a regional power in Latin America.[80]

Image 03: Infographic about cybersecurity scenario in Mexico.

Source: Center for Strategic and International Studies.[81]

[79]AGUILAR, Juan Antonio Manuel. **Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad**. URVIO – Revista Latinoamericana de Estudios de Seguridad, no. 25, pp. 24-40, Quito, Ecuador, 2019 December 19, 2015. Available at: http://scielo.senescyt.gob.ec/pdf/urvio/n25/1390-4299-urvio-25-00024.pdf. Accessed on: May 26, 2024.
[80]RODRIGUEZ-HERNANDEZ, Saúl Mauricio; VELÁSQUEZ, Nicolás. Mexico and cybersecurity: policies, challenges, and concerns. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 41, pp. 484-493.
[81]KOBEK, Luisa Parraguez. **The State of Cybersecurity in Mexico: An Overview**. Wilson Center, Washington, DC, 2017. Available at: https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview. Accessed on: May 26, 2024.

The absence of a digital mindset poses a significant obstacle even for Small and Medium-sized Enterprises (SMEs), contributing to a society that is negligent about cybersecurity measures.[82] While Mexico boasts significant potential for technological advancement, there remains a pressing need for improved political infrastructure and broader dissemination of digital knowledge.

Several strides have been made towards this transformation, particularly in regulating online illicit activities and advancing academic engagement. Notably, the National Association of Universities and Institutions of Higher Education (ANUIES) has led efforts through initiatives such as the National Computer Security Network (RENASEC). And lastly, a specialized Information and Communication Technology committee has been established to centralize discussion on cybersecurity issues.[83]

3.4 UNITED STATES OF AMERICA

When the Sputnik satellite was launched by the Soviet Union in September of 1957,[84] the United States Department of Defense (DoD) concluded it was necessary to consider ways information could still be disseminated even after a nuclear attack.[85] This culminated in the

[82]BERG, Ryan; ZIEMER, Henry. **The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment**. Center for Strategic and International Studies, Washington, DC, 2021 November 19. Available at: https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment. Accessed on: May 26, 2024.
[83]BERG, Ryan; ZIEMER, Henry. **The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment**. Center for Strategic and International Studies, Washington, DC, 2021 November 19. Available at: https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment. Accessed on: May 26, 2024.
[84]URI, J. **65 Years Ago: Sputnik Ushers in the Space Age - NASA.** Available at: https://www.nasa.gov/history/65-years-ago-sputnik-ushers-in-the-space-age/#:~:text=On%20Oct. Accessed on: March 30, 2024.
[85]UNIVERSITY SYSTEM OF GEORGIA. **A Brief History of the Internet.** Available at: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml. Accessed on: March 30, 2024.

creation of the Advanced Research Projects Agency Network (ARPANET), whose membership was limited to certain academic and research organizations who had contracts with the DoD. Eventually, ARPANET would evolve and become what today is known as the internet.[86]

The United States of America has had a long history of involvement in all types of cyber issues, ever since the dawn of cyber history. The Tor network – a free anonymizing overlay network commonly employed by users who wish to access the dark web[87] – bases itself on the core principle of onion routing, which was developed in the mid-1990s by United States Naval Research Laboratory (NRL) in order to protect U.S. intelligence communications online.[88]

With the creation of such base foundations for the cyber world, it is no marvel that the U.S. has such a heavyset presence on the discussion of cyber issues worldwide. The U.S. Department of Homeland Security (DHS) and its components play a major role in "strengthening cybersecurity resilience across the nation and sectors, investigating malicious cyber activity, and advancing cybersecurity alongside [the nation's] democratic values and principles".[89]

The most notable of these components is the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which leads the national effort to understand, manage, and reduce risk to cyber and physical infrastructure, while also being at the center of the exchange of cyber

---

[86]*Ibidem.*

[87]LAWRENCE, D. **Tor Anonymity Software vs. the National Security Agency - Businessweek**. Available at: https://web.archive.org/web/20140329174719/http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency. Accessed on: May 31, 2024.

[88]LEVINE, Y. **Almost everyone involved in developing Tor was (or is) funded by the US government**. Available at: http://pando.com/2014/07/16/tor-spooks/. Accessed on: May 31, 2024.

[89]DEPARTMENT OF HOMELAND SECURITY. **Cybersecurity**. Available at: https://www.dhs.gov/topics/cybersecurity. Accessed on: May 31, 2024.

defense information and defensive operational collaboration among the federal government, state, local, tribal and territorial (SLTT) governments, the private sector, and international partners.[90]

Moreover, the U.S. Science and Technology Directorate (S&T) frequently funds and conducts research, development, test and evaluation (RDT&E) of new technologies for usage in cybersecurity, vying to secure the nation's current and future cyber and critical infrastructures.[91] In doing so, it supports both internal DHS Components, such as CISA, and external federal agencies, such as the Federal Bureau of Investigations (FBI), with advanced critical infrastructure and cyber capabilities commonly developed through partnerships with national labs and stakeholders from the private sector. Private sector stakeholders include small businesses, international partners, law enforcement, industry, and academic groups.[92]

Cybersecurity regulation in the United States is divided between federal and state laws. At the federal level, the Federal Trade Commission (FTC) is responsible for enforcing cybersecurity regulations and legislation, basing itself upon the Federal Trade Commission Act (FTCA), a law that prohibits deceptive acts and practices in business, including those related to data security,[93] and The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, which outlaws conduct that victimizes computer systems.[94] The FTC also enforces the Gramm-

---

[90]*Ibidem.*

[91]DEPARTMENT OF HOMELAND SECURITY. **Cybersecurity / Information Analysis R&D | Homeland Security**. Available at: https://www.dhs.gov/science-and-technology/cybersecurity-information-analysis-rd. Accessed on: May 31, 2024.

[92]*Ibidem.*

[93]BRANDS, M. **Cybersecurity Laws and Legislation (2023) | ConnectWise**. Available at: https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation#:~:text=The%20primary%20law%20governing%20cybersecurity. Accessed on: May 31, 2024.

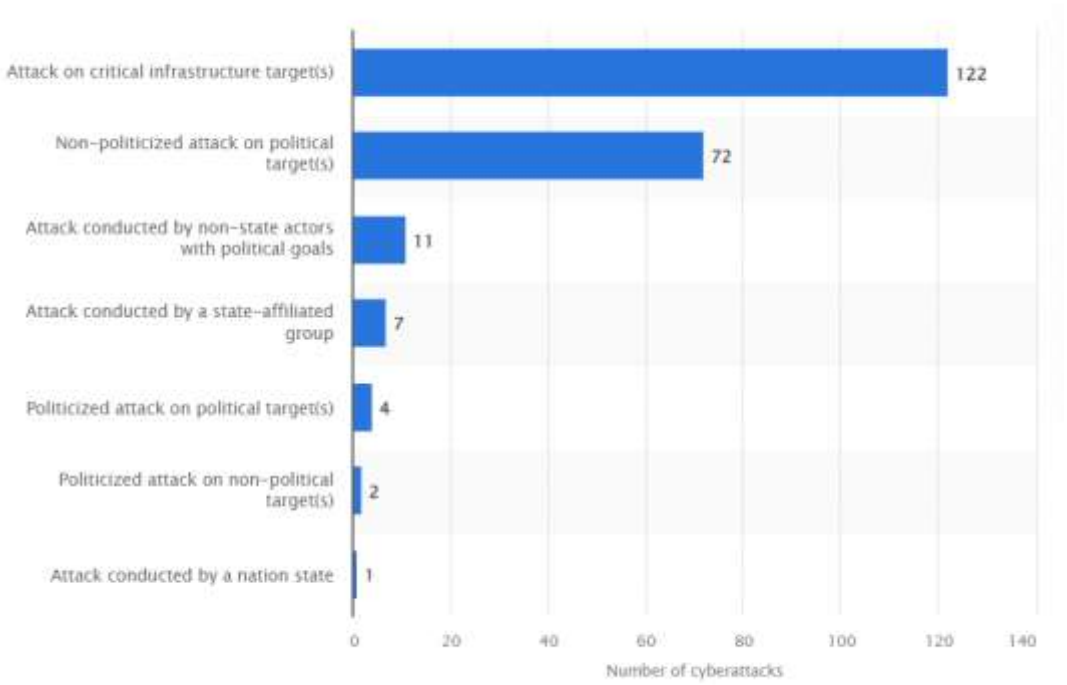
[94]DOYLE, C. **Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.** [s.l: s.n.]. Available at: https://crsreports.congress.gov/product/pdf/RL/97-1025#:~:text=The%20Computer%20Fraud%20and%20Abuse. Accessed on: May 31, 2024.

Leach-Bliley Act (GLB), which requires companies to protect the customer data they collect.[95]

Cybersecurity governance is carried out at the state level through regulations, legislations or statutes, and expenditures. However, only a few U.S. states had cybersecurity legislations or statutes in place that were funded, while the majority did not have a cybersecurity budget line item, and only 21% had it established by a statute or law.[96] Still, government databases are primary targets for hackers and acts of cyber warfare, and the frequency of data breaches, their complexity, and economic implications have increased.[97]

Image 04: Number of cyber incidents with a political dimension initiated against the United States in 2023, by attack characteristic.

[95]BRANDS, M. **Cybersecurity Laws and Legislation (2023) | ConnectWise**. Available at: https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation#:~:text=The%20primary%20law%20governing%20cybersecurity. Accessed on: May 31, 2024.
[96]PETROSYAN, A. **U.S. government and cybercrime - Statistics & Facts**. Available at: https://www.statista.com/topics/3387/us-government-and-cyber-crime. Accessed on: May 31, 2024.
[97]*Ibidem.*



Source: Statista.[98]

Examples of hacker attacks targeting government institutions as well as U.S.-based private companies are not few, and some, such as the 2018 United States Postal Service (USPS) data breach, exposed as many as 60 million data records. Other examples include the 2013[99] and 2014[100] Yahoo! data breaches, the first of which having affected all 3 billion users, and the 2021 Colonial Pipeline ransomware attack, caused gas supply shortages for Americans living in southeastern states.[101] Some attacks are also perpetrated as a form of hacktivism, such as the

[98] *Ibidem.*

[99] GOEL, V.; PERLROTH, N. **Yahoo Says 1 Billion User Accounts Were Hacked**. The New York Times, 14 dez. 2016. Available at: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html. Accessed on: May 31, 2024.

[100] STRETCH, B. **J. United States of America v. Dmitry Dokuchaev, Igor Sushchin, Alexey Belan, and Karim Baratov**, 28 fev. 2017. Available at: https://www.justice.gov/opa/press-release/file/948201/dl?inline. Accessed on: May 31, 2024.

[101] PRATT, M. **The 10 biggest ransomware attacks in history | TechTarget**. Available at: https://www.techtarget.com/searchSecurity/tip/The-biggest-ransomware-attacks-in-history. Accessed on: May 31, 2024.

data breach against one of the country's largest nuclear research facilities, the Idaho National Laboratory (INL) by a hacker collective of self-proclaimed "gay furry hackers"[102].

> meow meow meow meow meow meow meow [...] woah so much crunchy data **:3** [...] we're willing to make a deal with INL. if they research creating irl catgirls we will take down this post. [sic][103]

The collective, SiegedSec, affirmed that their decision to hack INL was not because of a specific political goal, but part of a general mission to damage the U.S. government, which they deem "one of the driving evil forces in the world."[104]

In 2013, a former U.S. computer contractor named Edward Snowden leaked thousands of classified documents (see section 6.4.1 of study guide) owned by the U.S. National Security Agency (NSA), one of the world's largest intelligence agencies.[105] Some of these documents detailed surveillance programs such as Prism, that would allegedly give the NSA direct access to emails, video chats and more from some of America's biggest tech companies.[106]

Additionally, the leaks also featured mentions of the Tailored Access Operations unit (TAO), a supposed special hacker force. According to national security reporter Jörg Schindler, the unit creates

---

[102]NAST, C. **"Gay Furry Hackers" Breached a Nuclear Lab to Demand Catgirl Research**. Available at: https://www.them.us/story/gay-furry-hackers-breached-nuclear-lab-catgirl-research-demand. Accessed on: May 30, 2024.
[103]*Ibidem.*
[104]*Ibidem.*
[105]VICE NEWS. **Exposing the NSA's Mass Surveillance of Americans | CYBERWAR**. Available at: https://www.YouTube.com/watch?v=tYVm62oEyWA. Accessed on: May 30, 2024.
[106]*Ibidem.*

tools to infiltrate, manipulate and sabotage every kind of digital device.[107] Not much is known about who TAO hacks, but the Snowden leaks reveal Osama Bin Laden as a main target. The unit hacked into mobile phones of Al-Qaeda operatives in the search for Bin Laden, as reported by the Washington Post, and its work also led to the capture of 40 insurgents in Afghanistan.[108] TAO is very entwined with and aims to facilitate military operations on the ground, tracking down targets who are subsequently captured or killed.[109]

Some of TAO's activities, however, seem to jeopardize internet security at large. As stated in a Snowden leak, TAO found a vulnerability in the Mozilla Firefox browser that helped them identify some users running anonymizing software Tor. In order to pull off this attack, the unit had to monitor and hijack internet traffic, and some hundreds of millions of Firefox users were left vulnerable in the meantime.[110]

Another important Snowden leak is known as the "Black Budget", which revealed that the NSA spends more than 600 million dollars a year for just the kind of offensive hacks TAO conducts.[111] According to hacker and anti-surveillance activist Claudio Guarnieri:

> The balance between how much is invested in breaking things and how much is invested in protecting things is uneven. Part of the mandate of intelligent services is to keep the country secure. However, from

[107] *Ibidem.*
[108] VICE NEWS. **Exposing the NSA's Mass Surveillance of Americans | CYBERWAR**. Available at: https://www.YouTube.com/watch?v=tYVm62oEyWA. Accessed on: May 30, 2024.
[109] *Ibidem.*
[110] *Ibidem.*
[111] *Ibidem.*

a technological perspective, they are undermining the security of the country.[112]

The NSA's elite hacking units have helped capture terrorists, but they have also targeted friendly nation states, as some Snowden leaks reveal. The elite unit has gone after Al-Qaeda and Taliban fighters, but the group has also hacked into the president of Mexico's emails and potentially aided the United Kingdom in spying a Belgian telecommunications company.[113]

In regards to cyberwarfare, the United States of America reserves the right to use military force in response to cyberattacks, as stated in the International Strategy for Cyberspace, published in 2011 by the White House.[114] While the responsibility for a cyberattack against another nation has never been officially claimed by the U.S. Government, it has been repeatedly accused of penetrating international systems, especially by Russia, China and Iran.[115] The Stuxnet virus – a virus that infiltrated and damaged Iranian nuclear power plants' systems, thus slowing down the country's nuclear program –, for example, is commonly attributed to the American and Israeli governments.[116]

Overall, the United States of America is one of the most powerful countries in the world when it comes to the cybersphere. As the birthplace of the internet and home to the Californian Silicon Valley, the

---

[112]*Ibidem.*

[113]*Ibidem.*

[114]THE WHITE HOUSE. **Prosperity, Security, and Openness in a Networked World**. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf. Accessed on: May 31, 2024.

[115]TIDY, J. **Why is it so rare to hear about Western cyber-attacks?** BBC News, 23 jun. 2023. Available at: https://www.bbc.com/news/technology-65977742. Accessed on: May 31, 2024.

[116]VICE NEWS. **The World's First Cyber Weapon Attack on a Nuclear Plant | Cyberwar**. Available at: https://www.YouTube.com/watch?v=dobTyPKccMA. Accessed on: May 30, 2024.

biggest agglomeration of high-tech industries in the world,[117] It is very much willing to work alongside UNODC to combat cybercrime. The U.S. has been a member of the UNODC ever since December 2003, having completed its ratification process in late 2006.[118]

[117]THE ECONOMIST. **Land of milk and start-ups.** Available at: http://www.economist.com/business/displaystory.cfm?story_id=10881264. Accessed on: May 31, 2024.
[118]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status**. Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 31, 2024.

4 ASIA

The Asian continent has always shown to be multifaceted culturally as an ancient territory which maintains an almost orthodox cultural heritage habits possibly leading to the increase of national afar discrepancies and a new ground zero when it comes jurisdictional shaping's of insidious crimes such as drug trafficking, child abuse and illicit content displays, the continent still has the biggest digital platforms, technological governmental projects billings with voluntary funding.[119]

Efforts have set forth pace and rising opportunities for a prosperous environment increasing organizations investing confidence and a highlighted realm for Research & Development as presented in the following collection.[120]

4.1 ISLAMIC REPUBLIC OF IRAN

The Islamic Republic of Iran has been part of the United Nations Office on Drugs and Crime since 2003, having completed the ratification of its protocols in 2008.[121] On the global stage, the country is central to the debate about the development of malicious digital technologies, being involved in numerous cyberattacks both as a victim and as an

[119]WORLD ECONOMIC FORUM. **Why is the Asia Pacific region a target for cybercrime - and what can be done about it?**. Available at: https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/. Accessed on: May 31, 2024.
[120]HFW. **The Rise Of Cybercrime In Asia Pacific And Considerations For Organisations Operating In The Region.** Available at: https://www.hfw.com/insights/The-rise-of-cybercrime-in-Asia-Pacific-and-Considerations-for-organisations-operating-in-the-region-August-2019/. Accessed on: May 31, 2024.
[121]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profile**: Iran (Islamic Republic of). 2024. Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Firn.html. Accessed on: May 27, 2024.

alleged perpetrator. Its conflict with the United States has already been titled "the first known cyberwar in history".[122]

Among the cyberattacks suffered by Iran, the Stuxnet case stands out, a self-replicating malware allegedly developed in co-authorship between the United States and Israel. Discovered by a Belarusian cybersecurity company in 2010, experts believe that the virus was developed to sabotage the Iranian nuclear program, altering discrete values, which were essential to the operation of the centrifuges at the Natanz uranium enrichment plant. It is estimated that the malware rendered more than 1000 Iranian nuclear centrifuges useless, delaying the country's nuclear program by at least 2 years.[123]

Driven by threats like Stuxnet, the Iranian government began to implement in 2013 the so-called National Information Network, a government intranet disconnected from the global internet. The implementation plan was divided into 2 stages: first limiting itself to operations and services in the public sector and then extending to other sectors of society. The network was fully implemented in 2019 and works, in practice, like the Great Chinese Firewall. Officially, the Iranian government claims that the National Information Network is an initiative to "break the internet monopoly".[124]

In summary, cyberwarfare is a central element of Iranian soft power, proving fundamental to the protection of its interests. Its main adversaries in this field are the United States (and by extension, its allies

---

[122]GROSS, Michaell Joseph. **Silent War**. Vanity Fair, June 6, 2013. Available at: https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business. Accessed on: May 27, 2024.

[123]BAEZNER, Marie; ROBIN, Patrice. **Stuxnet**. Center for Security Studies (CSS), ETH Zürich, Zurique, v. 4, October 18, 2017.

[124]CENTER FOR HUMAN RIGHTS IN IRAN. **The National Information Network (National Internet)**. Center For Human Rights in Iran, November 10, 2014. Available at: https://www.iranhumanrights.org/2014/11/internet-reportthe-national-information-network-national-internet/. Accessed on: May 27, 2014.

such as the United Kingdom[125], Turkey[126], and Albania[127], all alleged victims of Iranian cyberattacks) and Israel. Most of these offensive actions are taken not directly by the government, but by particular proxies like Crimson Sandstorm[128], independent parties allied with Iran on an ideologically or common enemy basis. With such predicament, the country ends up in an uncommon position where it both fights and funds independent hacker groups based on their alignments, always maintaining in public, however, a very combative stance against these illegal activities.

Over on the crime front, due to its geographic position, Iran is a major route for drug traffic, specially opioids and cannabis products fabricated in Afghanistan and Pakistan, acting as a pathway to Europe, Southeast Asia and the Persian Gulf.[129] Furthermore, although having strict laws against the commercialization of sex, the country has faced accusations of rampant sex trafficking among its marginalized populations, like refugees, migrants and LGBTQIAP+ people.[130]

---

[125]MACASKILL, Ewen. **Iran to blame for cyber-attack on MPs' emails – British intelligence**. The Guardian, October 14, 2017. Available at: https://www.theguardian.com/world/2017/oct/14/iran-to-blame-for-cyber-attack-on-mps-emails-british-intelligence#:~:text=Iran%20is%20being%20blamed%20for,comes%20at%20an%20awkward%20juncture. Accessed on: May 27, 2024.

[126]HALPERN, Micah. **Iran Flexes Its Power by Transporting Turkey to the Stone Age**. Observer, April 22, 2015. Available at: https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/. Accessed on: May 27, 2024.

[127]MAGID, Jacob; HOROVITZ, Michael. **Albania Cuts Diplomatic Ties With Iran, Boots Out Diplomats Over July Cyberattack**. The Times of Israel, September 7, 2022. Available at: https://www.timesofisrael.com/albania-cuts-diplomatic-ties-with-iran-boots-out-diplomats-over-july-cyberattack/. Accessed on: May 27, 2024.

[128]OPEN AI. **Disrupting malicious uses of AI by state-affiliated threat actors:** We terminated accounts associated with state-affiliated threat actors. Our findings show our models offer only limited, incremental capabilities for malicious cybersecurity tasks. OpenAi, February 14, 2024. Available at: https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/. Accessed on: May 27, 2024.

[129]CENTRAL INTELLIGENCE AGENCY. **The World Factbook:** Iran. Central Intelligence Agency, May 22, 2024. Available at: https://www.cia.gov/the-world-factbook/countries/iran/. Accessed on: May 27, 2024.

[130]*Ibidem.*

Iran does have an extensive and developed series of laws against cybercrimes, composed mainly of the Electronic Commerce Law 2004 (ECL), Cybercrime Law 2009, Civil Liability Act, and the Charter of Citizen's Rights. Together, these legal texts create a comprehensive network of protection against unauthorized distribution of data, breach of privacy, publication of illegal content, among others.[131]

The legal system, however, does face some international criticism when it comes to its cyberspace laws, with some of them being used to justify what international organisms consider censorship.[132] This, combined with the strong government control over the web provided by the National Information Network, has earned the country many denunciations of violation of freedom of speech.[133]

Overall, Iran stands as one of the most famous victims of cyber security threats, historically levering such a position to justify stronger control over the web and its own developments of cyberweapons.

4.2 ISLAMIC REPUBLIC OF PAKISTAN

The Islamic Republic of Pakistan became a member of the United Nations on September 30, 1947.[134] The country ratified the United

[131]FARD, Anahita Asgari. **E-commerce Law And Cybersecurity In Iran:** Nowadays, businesses are delegating more and more of their operations to the online arena, while the advertising and marketing activities are now predominantly conducted online, particularly on social networks. Mondaq, March 10, 2023. Available at: https://www.mondaq.com/privacy-protection/1291984/e-commerce-law-and-cybersecurity-in-iran. Accessed on: May 27, 2024.

[132]ARTICLE 19. **Islamic Republic of Iran:** Computer Crimes Law. Article 19, London, 2012.

[133]*Ibidem.*

[134]GOVERNMENT OF PAKISTAN. **United Nations.** Available at: https://unmissionnewyork.thaiembassy.org/en/content/53893-thailand-candidature-for-unsc?cate=5f2070fe71c05359785aa5ef. Accessed on: May 27, 2024.

Nations Convention against Corruption (UNCAC) on August 31, 2007, although the signature date was on December 9, 2003.[135]

When it comes to substantive law in the Islamic Republic of Pakistan, in 2016 The Prevention of Electronic Crimes Act was passed. It includes the following crimes: unauthorized access, copying, interference or transmission of information systems or data, glorification of offenses, cyber terrorism, and hate speech. Moreover, it also addresses recruitment, funding and planning of terrorism; electronic forgery; electronic fraud; making, supplying or obtaining devices for use in offense; identity crime; unauthorized interception, defamation; special protection of women; and, child pornography, as well as writing or distributing malicious code, cyberstalking, spamming and spoofing[136/137]

Furthermore, the Prevention of Electronic Crimes Act also provides for legal recognition of offenses committed in relation to information systems. In addition, the Pakistani Penal Code also includes pornography as an offense, while the Copyright Ordinance includes infringement of copyright.[138]

Nevertheless, according to Octopus Cybercrime Community, the Government of Pakistan has not yet adopted a cybercrime strategy. Although the Prevention of Electronic Crimes Act, 2016, is the main source of substantive law provisions, addressing in some form the majority of the offenses listed in the Budapest Convention, several powers are missing procedural conditions and safeguards.[139]

---

[135]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 23, 2024.
[136]A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.
[137]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 23, 2024.
[138]*Ibidem.*
[139]*Ibidem.*

Regarding international law, Pakistan cooperates with other countries based on being a member of Interpol however such cooperation is not efficient. Pakistan's Extradition Act governs the extradition process. Pakistan also has an extradition treaty in place with the United States of America which would be useful for cybercrime cases. Also, the Prevention of Electronic Crimes Act provides general international cooperation measures, including broad provisions relating to spontaneous information, grounds for refusal, confidentiality and limitation of use and enabling powers to cooperate with respect to specialized investigative measures.[140]

According to UNODC, The United Nations Office on Drugs and Crime (UNODC) in Pakistan, with the generous support of the United Nations Peace and Development Trust Fund (UNPDTF):

> (...) conducted a transformative series of training workshops aimed at enhancing Pakistan's counter-terrorism efforts. Across two workshops held from May 6th to 9th and May 13th to 16th, 2024 in Islamabad, UNODC equipped 44 analysts from the National Counter Terrorism Authority (NACTA) with cutting-edge skills in the utilization of Criminal Analysis Tools and techniques.[141]

In conclusion, Pakistan has developed a strong legislative framework to combat cybercrime through the Prevention of Electronic Crimes Act of 2016 and other relevant laws. However, the absence of a

[140]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 23, 2024.
[141]*Ibidem.*

comprehensive cybercrime strategy and certain procedural safeguards highlight areas for improvement. International cooperation, such as with Interpol and through UNODC training initiatives, plays a vital role in enhancing Pakistan's capabilities. Continued development and alignment with global standards are essential for effectively addressing cybercrime and related security issues.

4.3 KINGDOM OF SAUDI ARABIA

The Kingdom of Saudi Arabia has been part of the United Nations Office on Drugs and Crime since 2004, having completed the ratification of its protocols in 2013.[142] The main legislative force against cybercrime in the country consists of the Anti-Cyber Crime Law, composed of sixteen provisions that set out the key definitions, scope and objectives, sentences and fines in relation to cybercrimes.

The Saudi Anti-Cyber Crime Law looks to secure the safe exchange of data, protect the rights of users of the computers and the internet, and to protect the public interest and morals as well as people's privacy.[143] Brief and 17 years old, however, the law is considered outdated by modern standards, failing to protect against identity theft, invasion of privacy, cyber-bullying, among others.[144]

On an executive level, the kingdom has the National Cybersecurity Authority (NCA), an agency with both regulatory and

---

[142]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profile**: Iran (Islamic Republic of). 2024. Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Fsau.html. Accessed on: May 27, 2024.

[143]COUNCIL OF EUROPE. **Saudi Arabia**: Cybercrime policies/strategies. Council of Europe, 2020. Available at: https://www.coe.int/en/web/octopus/-/saudi-arabia. Accessed on: May 27, 2024.

[144]AISHAMMARI, Tareq Saeed; SINGH, Harman Preete. **Preparedness of Saudi Arabia to Defend Against Cyber Crimes**: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Boston University Press, Boston, October 30, 2023.

operational functions related to cybersecurity, working closely with public and private entities to improve the cybersecurity posture of the country.[145] The main action of the organism so far consists of establishing minimum standards of web security for the public bodies.[146]

It's important to note that Saudi Arabia is one of the most targeted nations globally by cybercriminals. The financial losses incurred by countries in the Gulf region due to cyberattacks rank among the highest worldwide. As per IBM's 2020 data, the average financial impact of a cyberattack on an organization in Saudi Arabia and the United Arab Emirates stood at $6.53 million. This figure is 69% higher than the global average.

According to the International Data Corporation (IDC) "Saudi Arabia's attractiveness to cybercriminals can be attributed to several factors, including the country's strategic importance, economic significance, political landscape, and abundant natural resources".[147]

With such predicament, the Kingdom is currently investing in a growing array of regulatory tools, toolkits, and guidelines. These have been recognized globally by the International Telecommunications Union's Global Cybersecurity Index, ranking Saudi Arabia in second place after the United States when it comes to ongoing cybersecurity investments.[148]

---

[145]COUNCIL OF EUROPE. **Saudi Arabia**: Cybercrime policies/strategies. Council of Europe, 2020. Available at: https://www.coe.int/en/web/octopus/-/saudi-arabia. Accessed on: May 27, 2024.

[146]SAUDI GAZETTE. **Follow basic cyber security standards, govt agencies told**. Saudi Gazette, October 07, 2018. Available at: https://saudigazette.com.sa/article/545053/SAUDI-ARABIA/Follow-basic-cyber-security-standards-govt-agencies-told. Accessed on: May 27, 2024.

[147]BULLER, Alicia. **Saudi Arabia Strengthens Its Cybersecurity Posture**. Dark Reading, December 28, 2023. Available at: https://www.darkreading.com/cyberattacks-data-breaches/saudi-arabia-strengthens-its-cybersecurity-posture. Accessed on: May 27, 2024.

[148]INTERNATIONAL TELECOMMUNICATIONS UNION. **Global Cybersecurity Index**. International Telecommunications Union, 2020. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed on: May 27, 2024.

Among these measures is the minting of the Personal Data Protection Law (PDPL), the first comprehensive data protection law in Saudi Arabia. Published in 2023, the legal text is expected to be fully implemented by September 2024, after a compliance period.[149]

Amid such rapid developments, the main difficulty faced by the country is the lack of qualified workforce. To this end, the Saudi government is investing heavily in initiatives to enhance digital skills, including a $1.2 billion plan to train 100,000 youths in fields like cybersecurity.[150]

In short, The Kingdom of Saudi Arabia has gained notoriety as having one of the fastest growing cybersecurity apparatuses. While still being an emerging potency on the field, the massive investments in it point out to a national policy compromised in updating the country's cybersecurity capabilities as fast as possible. To this effect, the greatest obstacle faced by the government is the lack of a specialized workforce. Apart from that, it’s indefeasible that the Kingdom comes from a history of being a major target of cyberattacks, a reality that only now is starting to change.

4.4 KINGDOM OF THAILAND

[149]MEENAGH, Brian A.; TUCKER, Lucy. **Six Months Until Enforcement**: Key Compliance Steps for Saudi Arabia’s Data Protection Law. Global Privacy & Security Compliance Law Blog, March 13, 2024. Available at: https://www.globalprivacyblog.com/2024/03/six-months-until-enforcement-key-compliance-steps-for-saudi-arabias-data-protection-law/. Accessed on: May 27, 2024.

[150]BULLER, Alicia. **Saudi Arabia Strengthens Its Cybersecurity Posture**. Dark Reading, December 28, 2023. Available at: https://www.darkreading.com/cyberattacks-data-breaches/saudi-arabia-strengthens-its-cybersecurity-posture. Accessed on: May 27, 2024.

The Kingdom of Thailand became a member of the United Nations on December 16, 1946.[151] The nation ratified the United Nations Convention against Corruption (UNCAC) only on March 1, 2011, although the signature date was on December 9, 2003.[152]

Regarding criminal laws that aim to prevent cybercrimes from occurring, the Kingdom of Thailand established the Computer Crime Act B.E 2550 in 2007. According to section 4: “the Minister of Information and Communications Technology shall have responsibility and control for the execution of this Act and shall have the authority to issue a Ministerial Rule for the purpose of the execution of this Act”.[153]

Furthermore, according to Section 9:

> (…) any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Finally, as stated by the Prime Minister:

> The rationale for the issue of this Act as of today is that a computer system is essential to business operations and the human way of life, as such, if any

[151]PERMANENT MISSION OF THAILAND TO THE UNITED NATIONS. **Thailand Candidature for UNSC.** Available at: https://unmissionnewyork.thaiembassy.org/en/content/53893-thailand-candidature-for-unsc?cate=5f2070fe71c05359785aa5ef. Accessed on: May 27, 2024.
[152]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 23, 2024.
[153]SAMUIFORSALE. **Computer Crime Act Criminal Law.** Available at: https://www.samuiforsale.com/law-texts/computer-crime-act.html#:~:text=Any%20person%20who%20illegally%20damages,hundred%20thousand%20baht%20or%20both. Accessed on: May 27, 2024.

> person commits an act that disables the working of a computer system according to the predetermined instructions or that causes a working error - a deviation from that required by the predetermined instructions or that resorts to any means to illegally know of, correct or destroy a third party's data contained in a computer system or that uses a computer system to disseminate false or pornographic computer data, then that act will damage and affect the country's economy, society and security including people's peace and good morals. Therefore, it is deemed appropriate to stipulate measures aimed at preventing and suppressing such acts. Hence the enactment of this Act.[154]

Concerning projects that the Kingdom of Thailand cooperates with the United Nations Office on Drugs and Crime (UNODC), currently it established an emergency response network to combat human trafficking in Southeast Asia, aiming to tackle the rising transnational criminality in the region. The network aims to enhance cooperation and coordination among law enforcement agencies, after the reunion that occurred in Bangkok, on May 15, 2024.[155]

The aforementioned project is major to provide better security in Southeast Asia. As stated by Rebecca Miller, Regional Coordinator for countering human trafficking and migrant smuggling at UNODC's Regional Office for Southeast Asia and the Pacific:

---

[154]*Ibidem.*

[155]UNODC REGIONAL OFFICE FOR SOUTHEAST ASIA AND THE PACIFIC. **Scams and trafficking for forced criminality: UNODC establishes an emergency response network to combat human trafficking in Southeast Asia.** Available at: https://www.unodc.org/roseap/en/2024/05/emergency-response-network/story.html. Accessed on: May 27, 2024.

> “In the last several years, Southeast Asia has faced unprecedented challenges from powerful transnational criminal groups involved in money laundering, cybercrimes, kidnapping, extortion, and torture,”[156]

In conclusion, Thailand has developed robust measures against cybercrime through the Computer Crime Act B.E 2550 of 2007 and by ratifying the UNCAC in 2011. The country actively collaborates with the UNODC, notably establishing an emergency response network to combat human trafficking in Southeast Asia. These initiatives are essential for enhancing national security and regional cooperation against transnational crimes. Continued efforts and international collaboration are crucial for addressing evolving cyber threats and criminal activities.

4.5 PEOPLE’S REPUBLIC OF CHINA

Since its accession to the Chinese seat in 1971,[157] The People’s Republic of China (PRC) has worked closely with the United Nations to promote domestic and international regulations to tackle criminality in all its forms, thus promoting a sustainable and safe development of its nation. This tight-knit relationship led the Office on Drugs and Crime to open an international headquarters in Beijing, an affair aimed specifically

[156] *Ibidem.*

[157] UNITED NATIONS. **Restoration of the lawful rights of the People's Republic of China in the United Nations.** UN: General Assembly, 1971. Available at: https://digitallibrary.un.org/record/192054?v=pdf. Accessed on: May 24, 2024.

at dealing with the issue of illicit drugs in the region, but whose limits of operations are much broader.[158]

Once the nation of the ingenious Four Great Inventions - the compass, gunpowder, paper-making and printing - and other important creations as silk and porcelain,[159] the Chinese government saw itself falling behind Western superpowers, and even its Japanese neighbors, in the development of technology throughout the 19th and 20th centuries. Furthermore, under Mao Zedong's power and the Cultural Revolution of the period, the concern with revolutionary purity was more prevalent than scientific progress, often coined as "taking the capitalist road", slowing down the country's technological expanse.[160]

Thus, with the desire to join in the competition, the post-Mao PRC devised several plans to further the country's industry and change the local perspective on scientists and researchers through the new media, starting from the 1970s, culminating in the 1986's State High-Tech Development Plan.[161] Mostly known as the 863 program (Chinese: 863计划), its goal was "to boost innovation capacity in the high-tech sectors",

[158]UNITED NATIONS. **United Nations Office on Drugs and Crime to Open Office in Beijing.** Vienna: UN Information Service, 2005. Available at: https://unis.unvienna.org/unis/en/pressrels/2005/unisnar920.html. Accessed on: May 24, 2024.
[159]HO, Mike. **The Four Great Inventions of Ancient China.** China: China Highlights, September 28, 2023. Available at: https://www.chinahighlights.com/travelguide/culture/four-great-invention.htm#other. Accessed on: May 26, 2024.
[160]WORDEN, R L; SAVADA, A M; DOLAN, R E. Science and Technology. In: WORDEN, R L; SAVADA, A M; DOLAN, R E. **China:** A Country Study. Washington, D.C.: Library of Congress, 1988. p. 371-406. Available at: https://www.loc.gov/item/87600493/. Accessed on: May 26, 2024.
[161]WORDEN, R L; SAVADA, A M; DOLAN, R E. Science and Technology. In: WORDEN, R L; SAVADA, A M; DOLAN, R E. **China:** A Country Study. Washington, D.C.: Library of Congress, 1988. p. 371-406. Available at: https://www.loc.gov/item/87600493/. Accessed on: May 26, 2024..

developing technologies to be used in both civilian and military endeavors.[162/163]

Alongside the financial backing of specific high-tech sectors, the country invested in higher education. Academic and research institutes were reopened, and young nationals were sent to attend universities and research institutes abroad, acquiring knowledge to later be put to use back in their homeland. It is estimated that over 35,000 students were sent to study in foreign countries, with 29,000 of those being sent to the United States between 1979 and 1986.[164]

From the change towards a market economy in 1978 to the present day, China has continued to dedicate time and effort to achieve technological advancement, both through their over 150,000 state-owned enterprises (SOEs) and the private sector.[165] In 2023, for instance, the country spent more than CNY 3.3 trillion (about USD 458.5 billion) in research and development of scientific and technological innovations, with four of its companies making to the top 50 R&D investors ranking[166] and placing 12th in the Global Innovation Index (GII), an index to track

---

[162]MINISTRY OF SCIENCE AND TECHNOLOGY OF THE PEOPLE'S REPUBLIC OF CHINA. **National High-tech R&D Program (863 Program).** Beijing: Ministry of Science and Technology of the People's Republic of China. Available at: https://en.most.gov.cn/programmes1/. Accessed on: May 26, 2024.

[163]RASKA, Michael. **Scientific Innovation and China's Military Modernization.** Arlington: The Diplomat, September 3, 2023. Available at: https://thediplomat.com/2013/09/scientific-innovation-and-chinas-military-modernization/. Accessed on: May 26, 2024.

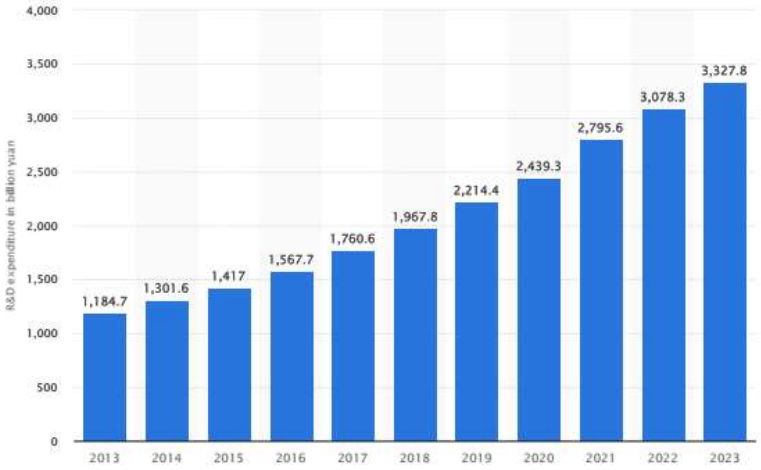
[164]WORDEN, R L; SAVADA, A M; DOLAN, R E. Science and Technology. In: WORDEN, R L; SAVADA, A M; DOLAN, R E. **China**: A Country Study. Washington, D.C.: Library of Congress, 1988. p. 371-406. Available at: https://www.loc.gov/item/87600493/. Accessed on: May 26, 2024.

[165]FENG, Jenny. **Government-backed and infrastructure-oriented: The Chinese way of innovation**. Suzhou: The China Project, March 28, 2023. Available at: https://thechinaproject.com/2023/03/28/government-backed-and-infrastructure-oriented-the-chinese-way-of-innovation/. Accessed on: May 26, 2024.

[166]STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA. **China's R&D expenditure exceeds 3.3 trln yuan in 2023: minister**. Beijing: The State Council of The People's Republic of China, March 5, 2024. Available at: https://english.www.gov.cn/news/202403/05/content_WS65e6ff4dc6d0868f4e8e4b66.html. Accessed on: May 26, 2024.

global innovation trends and intellectual property registrations around the globe.[167]

Image 05: China's R&D expenditure in billion yuan.



Source: Statista.[168]

Contrary to the PRC's initial socialist ideology, three of the four aforementioned companies appearing in top 50 R&D investors are private. The world's largest telecommunication supplier, Huawei Investment and Holding, listed in the top 5 of the European Commission's publication, claims to have invested more than CNY 1.1 billion over the last decade, with a policy to invest a minimum 10% of its yearly sales revenue into R&D,[169] amassing to an amount of around CNY

[167]WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **Global Innovation Index:** Innovation in the face of uncertainty. Geneva: WIPO, 2024. Available at: https://www.wipo.int/global_innovation_index/en/. Accessed on: May 26, 2024.
[168]TEXTOR, C. **Total expenditure on research and development (R&D) in China from 2013 to 2023**. Statista, May 24, 2024. Available at: https://www.statista.com/statistics/279951/internal-research-and-development-expenditure-in-china/. Accessed on: May 26, 2024.
[169]HUAWEI. **2023 Annual Report.** Shenzhen: Huawei, 2023. Available at: https://www.huawei.com/en/annual-report/2023. Accessed on: May 26, 2024.

15 billion, as the Shenzhen-based company aims to become the global leader in 5G technology.[170]

Additionally, China's second largest R&D spender Tencent Holdings funded CNY 150 billion between 2020 and 2022 in the sector,[171] while Alibaba Group Holding, placed third domestically and 22nd worldwide, had over EUR 5 billion in spendings in 2022 according to the European study.[172] Both corporations seem to be venturing in AI development,[173] as China has plans to match the investment of world leaders in the field by 2020, to surpass them and become the sole world leader in AI technology by the year 2030.[174]

Amongst relevant PRC's plans to propel the socio-economic sphere is the Internet Plus Initiative. Released in 2015, the initiative aims to use the Internet and its related technologies as a tool to enhance the economy "deepening the integration of the Internet, cloud computing, and big data into traditional manufacturing",[175] thus, hoping to, by 2025, become a driving force in the Chinese economy.[176]

---

[170]REUTERS. **Huawei to raise minimum annual R&D spending to at least US$15 billion.** Hong Kong: South China Morning Post, July 26, 2018. Available at: https://www.scmp.com/tech/social-gadgets/article/2157024/huawei-raise-minimum-annual-rd-spending-least-us15-billion. Accessed on: May 26, 2024.

[171]TENCENT. **#TencentInnovates: 8 Ways Tencent is Innovating to Make a Difference for People.** Shenzhen: Tencent, July 26, 2023. Available at: https://www.tencent.com/en-us/articles/2201654.html. Accessed on: May 26, 2024.

[172]NINDL, Elisabeth. *et al.* **The 2023 EU Industrial R&D Investment Scoreboard.** Luxembourg: Publications Office of the European Union, 2023. Available at: https://dx.doi.org/10.2760/506189. Accessed on: May 26, 2024.

[173]XINHUA. **China's internet giants report rapid Q3 growth amid innovation drive.** Beijing: Xinhua, November 24, 2023. Available at: https://english.news.cn/20231124/04448902836e4526ba69c8d7489b2d42/c.html. Accessed on: May 26, 2024.

[174]JIA, Denise; ZHANQUI, Ye. **China Outlines Ambitions to Become World Leader in AI by 2025**. Beijing: Caixin Global, July 21, 2017. Available at: https://www.caixinglobal.com/2017-07-21/china-outlines-ambitions-to-become-world-leader-in-ai-by-2025-101119663.html. Accessed on: May 27, 2024.

[175]DAVIDSON, Lincoln E. **'Internet Plus' and the Salvation of China's Rural Economy**. Arlington: The Diplomat, July 17, 2025. Available at: https://thediplomat.com/2015/07/internet-plus-and-the-salvation-of-chinas-rural-economy/. Accessed on: May 27, 2024.

[176]XINHUA. **China unveils Internet Plus action plan to fuel growth.** Beijing: The State Council of The People's Republic of China, July 4, 2025. Available at: http://english.www.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm. Accessed on: May 27, 2024.

Since its first connection to the World Wide Web (WWW) in 1994, the Internet has spread its reach in this East-Asian nation. According to the World Bank, there are over 1 billion Sino-internet-users, a penetration of 76% of the country's entire population with Internet access, making it the world's largest Internet user base.[177/178] Along with its increasing user base, e-commerce has become one of China's most lucrative ventures and one of the Chinese's favorite pastime activities, as they average almost 30 minutes a day scrolling through e-commerce platforms like Alibaba's Taobao, JD.com and others.[179]

With this many people with access to the web, the Chinese Communist Party (CCP) had to carefully craft mechanisms to control and regulate the activity of natural people and private/public organizations. Although the country's Constitution and its Civil Code already brought guarantees to privacy and the protection of personal information, further laws were necessary to tackle the specifics of the online world. Thus, were birthed the triarchy of Chinese cybersecurity regulations: the Cybersecurity Law (CSL) of 2017, and the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) of 2021.[180]

The first of its kind, the CSL proposes the fundamentals for cyberspace regulations. It imposes the role to manage and monitor all of one's data network, and of storing all logs and relevant information - gathered or produced in the country or belonging to a Chinese citizen -

[177]CHINA POWER TEAM. **How Web-connected is China?.** China Power, April 18, 2019. Available at: https://chinapower.csis.org/web-connectedness/. Accessed on: May 27, 2024.
[178]THE WORLD BANK. **China.** Washington, DC: The World Bank Group, 2024. Available at: https://data.worldbank.org/country/china#:~:text=Individuals%20using%20the%20Internet%20(%25%20of%20population). Accessed on: May 27, 2024.
[179]CHINA POWER TEAM. **How Web-connected is China?.** China Power, April 18, 2019. Available at: https://chinapower.csis.org/web-connectedness/. Accessed on: May 27, 2024.
[180]LUO, Dora; WANG, Yanchen. **China - Data Protection Overview.** Beijing: OneTrust DataGuidance, October, 2023. Available at: https://www.dataguidance.com/notes/china-data-protection-overview. Accessed on: May 27, 2024.

for a period of at least six months within mainland territory. These regulations are challenging in particular to small-sized and foreign companies that have to spend extra on either a new data server or hiring a local provider.[181]

Internationally, there's also the concern that, having placed its data in a Chinese server, the government may request access to a company's intellectual property. Article 28 of the CSL states that "network operators shall provide technical support and assistance to public security organs' and state security organs' lawful activities preserving national security and investigating crimes".[182] The article, and most of the law, may be considered as vague, leaving enterprises unaware of what reasons the CCP government could possibly use to request access to their data.[183/184]

Moreover, coming into effect two months off each other, the DSL and the PIPL are focused on the misuse and categorization of personal data. With those laws, Chinese nationals can be required to access, correct and delete their personal data in the hands of any business, while said businesses must classify their gathered data accordingly and are

[181]WAGNER, Jack. **China's Cybersecurity Law: What You Need to Know.** Arlington: The Diplomat, June 01, 2017. Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/. Accessed on: May 27, 2024.
[182]CHINA LAW TRANSLATE. **2016 Cybersecurity Law.** November 07, 2016. Available at: https://www.chinalawtranslate.com/en/2016-cybersecurity-law/. Accessed on: May 27, 2024.
[183]WAGNER, Jack. **China's Cybersecurity Law: What You Need to Know.** Arlington: The Diplomat, June 01, 2017. Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/. Accessed on: May 27, 2024.
[184]RUAN, Lotus. **What Does China's New Cybersecurity Law Mean for Chinese Internet Companies?.** Arlington: The Diplomat, November 10, 2016. Available at: https://thediplomat.com/2016/11/what-does-chinas-new-cybersecurity-law-mean-for-chinese-internet-companies/. Accessed on: May 27, 2024.

now to request the Cyberspace Administration of China's (CAC) approval to pursue a number of activities with its acquired information.[185/186]

Although no particular legislation has been made to tackle cybercrime, changes in the Criminal Code have, and new guidelines are not discarded to come in the future.[187] The People's Republic of China has proven interest and caution with the cyber world, proposing development and learning in and within the internet to guarantee a safe experience to its citizens. Now, all that remains is to join its forces with other international sovereigns to expand security and privacy on the internet to all beings in the world.

4.6 REPUBLIC OF INDIA

The Republic of India is one of the 51 founding members of the United Nations, having ratified the United Nations Convention against Corruption (UNCAC) on May 9, 2011, although the signature date was on December 9, 2003. The Convention covers five main areas: preventive measures, criminalization and law enforcement, international cooperation, asset recovery, and technical assistance and information exchange, also some of the goals of UNODC.[188]

---

[185]CHEN, Chi; ZHOU, Leo. **Global companies must assess their data compliance maturity levels and determine whether processes can be improved.** Shanghai: Ernst & Young, July 18, 2022. Available at: https://www.ey.com/en_gl/insights/forensic-integrity-services/how-chinas-data-privacy-and-security-rules-could-impact-your-business#:~:text=The%20Personal%20Information%20Protection%20Law,(DSL)%20came%20into%20force. Accessed on: May 27, 2024.

[186]LUO, Dora; WANG, Yanchen. **China - Data Protection Overview.** Beijing: OneTrust DataGuidance, October 2023. Available at: https://www.dataguidance.com/notes/china-data-protection-overview. Accessed on: May 27, 2024.

[187]LUO, Dora; WANG, Yanchen. **China - Data Protection Overview.** Beijing: OneTrust DataGuidance, October 2023. Available at: https://www.dataguidance.com/notes/china-data-protection-overview. Accessed on: May 27, 2024.

[188]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 23, 2024.

The Information Technology (IT) Act, 2000, is the primary legislation in the Republic of India dealing with cybersecurity, data protection and cybercrime. It provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.[189] For instance, some of its key features are identifying activities such as hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft as punishable offenses, and also to safeguard electronic data, information and records, aiming to protect computers systems.[190]

Moreover, the Indian Penal Code (IPC), firstly passed in 1860, was edited to contain cybersecurity-related provisions, which punishes offenses committed in cyberspace, such as defamation, cheating, criminal intimidation and obscenity.[191] The federal government, through the National Cyber Security Coordinator, is formulating a new national cybersecurity strategy. This aims to address certain gaps in India's cybersecurity framework and enhance the country's overall cybersecurity posture.[192]

Furthermore, the IPC also aims to protect children online. According to Section 293, it provides for provision against the sale or distribution of obscene objects to any child who is under the age of majority. Although, it is still considered to be limited, with lack of any

[189]PWC. **A comparison of cybersecurity regulations: India.** Available at: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india. Accessed on: May 23, 2024.
[190]PWC. **A comparison of cybersecurity regulations: India.** Available at: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india. Accessed on: May 23, 2024.
[191]*Ibidem.*
[192]*Ibidem.*

serious laws that effectively address and combat heinous crimes such as sexual exploitation and sexual abuse.[193]

The Indian Courts, in many landmark judgments, have provided necessary instructions for safeguarding minors against sexual abuse. In a case in Bombay High Court, various guidelines, for instance to block pornographic websites, have proper rules in cyber cafes so that the children cannot access the unsuitable material and no such content would be distributed in these cafes which is inappropriate for the children.[194]

A project combining UNODC, the Ministry of Social Justice and Empowerment (MSJE), Government of India and the Departments of Social Justice in Assam and Manipur, conducted a three-day training for 39 government representatives, social workers, teachers, psychologists, and community leaders from Assam and Manipur. The training equipped participants with knowledge and skills to effectively empower families and protect young people from the dangers of drugs and crime.[195]

In conclusion, India has established a strong legal framework to combat cybercrime through the IT Act, 2000, and the Indian Penal Code, with ongoing efforts to enhance cybersecurity via a new national strategy. The country's ratification of the UNCAC and collaboration with UNODC reflect its commitment to international standards and regional cooperation. These measures, along with landmark court judgments and

[193]SUMEDHA, GUPTA. **Child Pornography and Internet Subcultures in India - a Legal Perspective.** Available at: file:///E:/Downloads/Child_Pornography_and_Internet_Subcultures_in_Indi.pdf. Accessed on May 23, 2024.

[194]*Ibidem.*

[195]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **India: UNODC initiative focuses on empowering families to protect young people from drugs and crime.** Available at: https://www.unodc.org/southasia/en/frontpage/2024/February/india_-unodc-initiative-focuses-on-empowering-families-to-protect-young-people-from-drugs-and-crime.html. Accessed on: May 23, 2024.

community training initiatives, are crucial for protecting citizens, especially minors, from cyber threats.

4.7 REPUBLIC OF THE PHILIPPINES

The Philippines - officially the Republic of the Philippines - is one of the original 51 Founding Members of the United Nations that signed the UN Charter on June 26, 1945.[196] The UN Country Team (UNCT) in the Philippines consists of eleven resident funds, programs, and specialized agencies, six project offices, five non-resident agencies, and four UN Secretariat offices.[197]

Furthermore, ratified the United Nations Convention against Corruption (UNCAC) on November 8, 2006, although the signature date was on December 9, 2003.[198] UNCAC is the only legally binding universal anti-corruption instrument. Five main areas are covered by the Convention: criminalization and law enforcement, international cooperation, preventive measures, asset recovery, and technical assistance and information exchange.[199]

On January 19, 2016, the Philippines became the next country in Association of Southeast Asian Nations (ASEAN) – a political and economic union of 10 states in Southeast Asia. – to formally join the United Nations Office on Drugs and Crime (UNODC) - World Customs

[196]UNITED NATIONS PHILIPPINES. **United Nations in the Philippines.** Available at: https://philippines.un.org/en/about/about-the-un. Accessed on: May 18, 2024.
[197]*Ibidem.*
[198]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 18, 2024.
[199]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **United Nations Convention against Corruption.** Available at: https://www.unodc.org/unodc/en/treaties/CAC/. Accessed on: May 18, 2024.

Organization (WCO).[200] The mission of the UNODC-WCO Container Control Programme (CCP) is to build capacity in countries seeking to improve risk management, supply chain security, and trade facilitation in seaports, airports and land border crossings in order to prevent the cross-border movement of illicit goods.[201]

The Global Container Control Programme is a joint initiative of the United Nations Office on Drugs and Crime (UNODC) and the World Customs Organization (WCO). Launched in 2004 in response to the organized crime and human security threats posed by the maritime movement of illicit goods in sea containers, the Programme operates through the establishment of specialized Port Control Units (PCUs) securing the global supply chain.[202]

Moreover, The United Nations Office of Counter-Terrorism (UNOCT) and the United Nations Office on Drugs and Crime (UNODC), in association with the Government of the Philippines, launched the project “Technical support on the rights and needs of victims of terrorism through the Model Legislative Provisions and the development of National Comprehensive Assistance Plans”.[203]

The launch of the project in the Philippines is an important milestone in the international victims of terrorism agenda, as it marks the first time that a Member State takes action to implement the Model Legislative Provisions to Support the Rights and Needs of Victims of

---

[200]UNODC Regional Office for Southeast Asia and the Pacific. **The Philippines joins the UNODC-WCO Container Control Program.** Available at: https://www.unodc.org/roseap/en/2016/01/wco-ccp/story.html. Accessed on: May 18, 2024.

[201]UNODC REGIONAL OFFICE FOR SOUTHEAST ASIA AND THE PACIFIC. **The Philippines joins the UNODC-WCO Container Control Program.** Available at: https://www.unodc.org/roseap/en/2016/01/wco-ccp/story.html. Accessed on: May 18, 2024.

[202]*Ibidem.*

[203]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **United Nations and Philippines Launch New Project to Support Victims of Terrorism Through Legislative Frameworks.** Available at: https://www.unodc.org/unodc/en/terrorism/latest-news/2024_unodc_united-nations-and-philippines-launch-new-project-to-support-victims-of-terrorism-through-legislative-frameworks.html. Accessed on: 18 May, 2024.

Terrorism, while also responding to General Assembly resolution 35/705, which calls on member states to develop national comprehensive assistance plans.[204]

The CyberSecurity Philippines CERT is a non-profitable Computer Security Incident Response Team (CSIRT), which is a service organization responsible for receiving, reviewing, and responding to computer security incident reports and activities, to the purpose of study and solve problems with widespread cybersecurity implications, conduct research & development and provide advisories on security compromises under the Philippines Autonomous System Number (ASN).[205]

As a certified CSIRT, the Cybersecurity Philippines, CERT helps respond to breaches and act as subject matter experts to detect, respond, and secure networks from various compromises. For the purpose of determining techniques and tactics of attackers such as lateral movement, data exfiltration, insider threat, network, mobile, and web application attacks, even if they try to use anti-forensics techniques.[206]

The CSIRT provides the root cause analysis of the incident and determines the capabilities of the tools used by the attacker, either malware or scripts leveraging the operating system used. By learning the hacker´s strategy, it becomes easier to determine the steps required for proper planning and remediation. Eventually, elevating the stage of the user´s cyber resiliency.[207]

---

[204]*Ibidem.*

[205]CYBERSECURITY PHILIPPINES CERT. **A credible and trusted leader in Cybersecurity.** Available at: https://cert.ph/. Accessed on: 18 May, 2024.

[206]CYBERSECURITY PHILIPPINES CERT. **Digital Forensics and Incident Response.** Available at: https://cert.ph/digital-forensics-incident-response. Accessed on: May 18, 2024.

[207]*Ibidem.*

According to the Department of Justice - Office of Cybercrime of the Philippines (OOC) - Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 created OOC within the DOJ and designated it as the Central Authority in all matters relating to international mutual assistance and extradition for cybercrime and cyber-related matters. [208]

The section 2 of the Act No. 10175 - an act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefore and for other purposes. It highlights that the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.[209]

According to the fourth section of the Act. No. 10175, offenses against confidentiality, integrity and availability of computer data and systems such as: illegal access, illegal interception, data interference, system interference and the misuse of devices and cyber-squatting are punishable under the act.[210] Alongside those infractions, so are other computer-related offenses, for instance; computer-related forgery, computer-related fraud and computer-related identity theft, as well as content-related offenses such as cybersex, child pornography, unsolicited commercial communications and libel.

Lastly, the last category also introduces aiding or abetting in the commission of cybercrime and attempting to commit any of these offences in the commission of cybercrime.[211]

---

[208]DEPARTMENT OF JUSTICE, OFFICE OF CYBERCRIME. **Republic Act No. 10175.** Available at: https://cybercrime.doj.gov.ph/. Accessed on: May 20, 2024.

[209]DEPARTMENT OF JUSTICE, OFFICE OF CYBERCRIME. **Republic Act No. 10175.** Available at: https://cybercrime.doj.gov.ph/republic-act-no-10175-cybercrime-prevention-act-of-2012/. Accessed on: May 20, 2024.

[210]*Ibidem.*

[211]*Ibidem.*

Regarding international cooperation, section 22 of the Act No. 10175 implies that all relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal, offense shall be given full force and effect.[212]

Nevertheless, the Republic of the Philippines is seen by rights groups as the epicenter of the growing trade, which they say has been fueled by access to cheap internet and technology, the high level of English, well-established money wiring services and rampant poverty. Receiving at least 3,000 reports per month from other countries of possible cases of its children being sexually exploited online - a number which has tripled in the last three years - according to its justice department.[213]

Image 06: Detailed assessment of criminality in the Philippines.

[212] *Ibidem.*

[213] GUILBERT, Kieran. **Webcam Slavery: Tech turns Filipino families into cybersex child traffickers.** Available at: https://www.reuters.com/article/us-philippines-trafficking-technology/webcam-slavery-tech-turns-filipino-families-into-cybersex-child-traffickers-idUSKBN1JE00X/. Accessed on: May 20, 2024.

Source: Global Organized Crime Index.[214]

As to the criminal markets of the Philippines, such as human trafficking, human smuggling, extortion and protection racketeering, arms trafficking, illicit trade, illegal logging and flora and wildlife trafficking, illegal mining, drug smuggling, financial crimes and finally, cybercrime -

[214]ENACT. **Global Organized Crime Index - Philippines.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_philippines_2023.pdf. Accessed on: May 20, 2024.

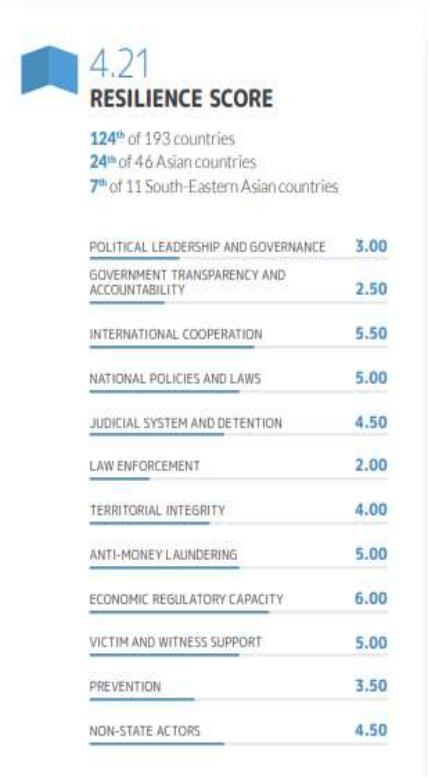
ranking among the most affected countries worldwide in terms of the number of cyber-attacks and threats.[215]

The COVID-19 pandemic has increased the use of digital platforms and the dark web for drug trafficking, especially for synthetic drugs. Efforts to counter the narcotics trade in the country are undermined by systemic corruption at all levels of state institutions. The government of the Philippines is criticized for its questionable conduct to prevent crimes.[216]

The judicial system of the Philippines is known for its unclear stance on anti-crime efforts, with evidence of widespread links between organized crime, politics and state institutions in the Philippines. Moreover, law enforcement in the Philippines remains fragile, with law enforcers, especially customs, border and maritime officials, frequently accused of corruption.[217]

Image 07: Detailed assessment of the resilience score for the Philippines.

[215]ENACT. **Global Organized Crime Index - Philippines.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_philippines_2023.pdf. Accessed on: May 20, 2024.
[216]*Ibidem.*
[217]*Ibidem.*



Source: Global Organized Crime Index.[218]

According to section 2 of the Republic Act No. 10175, the State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation's overall social and economic development.

The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information. It also frames the need to protect and safeguard the integrity of computer and communications systems, networks, and databases, and the confidentiality, integrity, and

[218]ENACT. **Global Organized Crime Index - Philippines.** Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_philippines_2023.pdf. Accessed on: May 20, 2024.

availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts.[219]

4.8 STATE OF ISRAEL

The State of Israel has been part of the United Nations Office on Drugs and Crime since 2005, having completed the ratification of its protocols in 2009. In recent years, Israel has emerged as a hub for cybersecurity expertise, with a strong focus on combating cyber threats. The demand for skilled professionals in this field remains high due to the ongoing challenges posed by cyber warfare and criminal activities.

According to the IVC Research Center, Tel Aviv witnessed 23 exits[220] of cybersecurity companies in 2021, making it a standout sector in the city's high-tech landscape. These exits included significant deals such as mergers and acquisitions, highlighting the industry's value. Furthermore, in 2021, the total number of active Israeli cybersecurity companies amounted to 469. These firms offer a wide range of protective solutions, particularly in data security, developing VPNs, Firewalls, and other advanced solutions. Projections indicate that the country's cybersecurity revenue will reach $1.43 billion by 2028.[221]

Having ratified the Budapest Convention on Cybercrime in 2016, Israel has incorporated all of its main terms in their penal code, criminal

---

[219]DEPARTMENT OF JUSTICE, OFFICE OF CYBERCRIME. **Republic Act No. 10175.** Available at: https://cybercrime.doj.gov.ph/republic-act-no-10175-cybercrime-prevention-act-of-2012/. Accessed on: May 21, 2024.

[220]In business, an "exit" is the moment when the partner or investor sells their stake in the business. For startups, this is most anticipated by those who invest in them (especially the entrepreneur), as the person receives a return on their investment and effort. In practice, an exit usually means that the business either went public, selling its stakes over on the stock market, or was sold to another company.

[221]LICHTER, Eyal. **Cybersecurity in Israel**: statistics & facts. Statista, December 21, 2023. Available at: https://www.statista.com/topics/10918/cybersecurity-in-israel/#topicOverview. Accessed on: May 27, 2024.

procedure law and computers Act (1995). To enforce the legislation, the country boasts its own National Cyber Directorate, a regulatory and supervisory body created in 2017 from the merger of the National Cyber Headquarters and the National Cyber Authority. On matters of Privacy protection, in 2006 The Ministry of Justice founded the Israeli Law, Information and Technology Authority. Finally, the Israeli police also has its own cybercrime division.[222]

Statistically wise, the most common cybercrimes experienced by the Israelis are unauthorized distribution of information and identity theft, each representing more than a third of all illicit cyber activity witnessed by the country.[223]

An interesting fact to note, over the past weeks, Check Point Research (CPR) has observed an 18% increase in cyberattacks on targets in Israel compared to before the October 7th attacks and the escalation of the Israeli-Hamas conflict; in addition, the Government/Military sector have seen a 52% increase in the number of cyber attacks compared to the average for the weeks prior to October 7th. The overall trend in this specific sector shows a decrease of 4% over the same period worldwide.[224]

Moreover, a key factor when it comes to Israel and the R&D of malicious technology is the case of Stuxnet: a self-replicating malware allegedly developed in co-authorship between the United States and Israel. Discovered by a Belarusian cybersecurity company in 2010,

---

[222]COUNCIL OF EUROPE. **Israel**: Status regarding Budapest Convention. Council of Europe, 2024. Available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/israel/. Accessed on: May 27, 2024.

[223]LICHTER, Eyal. **Share of cybercrime incidents among individuals in Israel in 2021, by type**. Statista, March 26, 2024. Available at: https://www.statista.com/statistics/1371721/share-of-cybercrime-incidents-among-individuals-in-israel-by-type/. Accessed on: May 27, 2024.

[224]SECURITY REPORT. **Análise laboratorial indica alta nas atividades cibernéticas contra aliados de Israel**. Security Leaders, November 3, 2023. Available at: https://securityleaders.com.br/analise-laboratorial-indica-alta-nas-atividades-ciberneticas-contra-aliados-de-israel/. Accessed on: May 27, 2024.

experts believe that the virus was developed to sabotage the Iranian nuclear program, altering discrete values, which were essential to the operation of the centrifuges at the Natanz uranium enrichment plant.[225]

It is estimated that the malware rendered more than 1000 Iranian nuclear centrifuges useless, delaying the country's nuclear program by at least 2 years.[226] Neither Israel nor the United States have ever acknowledged their authorship of the virus, but it has been exhaustively claimed by the media since its discovery.[227]

In conclusion, the State of Israel represents a powerhouse in cybersecurity, boasting billionaire revenues in the sector. Such a position, however, throws the country under intense international scrutiny when it comes to the development of malicious technologies, as shown by the Stuxnet allegations. Furthermore, the recent intensification of its war with Hamas has increased the number of cyberattacks suffered by the State, presumably by the terrorist organization, rendering cyberspace as one of the conflict’s fronts.

[225] BAEZNER, Marie; ROBIN, Patrice. Stuxnet. Center for Security Studies (CSS), ETH Zürich, Zurique, v. 4, October 18, 2017.
[B] *Ibidem.*
[227] HALLIDAY, Josh. **Stuxnet worm is the 'work of a national government agency'**. The Guardian, September 24, 2010. Available at: https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency/. Accessed on: May 27, 2024.

5 EUROPE

With an internet penetration of over 90%,[228] Europe has been one of the most proactive continents in the cybersecurity sphere. Having established its own agency focused on the matter, the European Union Agency for Cybersecurity (ENISA), as early as 2004,[229] it has developed an expressive number of guides and regulations pertaining to the subject of user safety on the web, like the EU Cybersecurity Act, the Budapest Convention on Cybercrime and the General Data Protection Regulation (GDPR). In addition, some of these conventions are not limited to European countries alone, making the region a global leader when it comes to safeguarding the very prevalent connected lives of the world population.[230/231]

When it comes to research and development of new technologies, the continent scores higher than the global average, with an estimated 2.24% of GDP spent in 2022.[232] Europe as a whole also heavily incentives companies and governments alike to invest in the sector, with many nations in this block with relevant corporations in the world leaderboard for R&D spending and a growing interest in new tech, such as AI.[233] Germany, for example, has eight companies in the top 50,

---

[228]EUROSTAT. **Digital economy and society statistics - households and individuals.** April, 2024. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals. Accessed on: May 31, 2024.
[229]EUROPEAN UNION AGENCY FOR CYBERSECURITY. **About ENISA - The European Union Agency for Cybersecurity.** Available at: https://www.enisa.europa.eu/about-enisa. Accessed on: May 31, 2024.
[230]EUROPEAN COMISSION. **Data protection in the EU.** Available at: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en. Accessed on: May 31, 2024.
[231]COUNCIL OF EUROPE. **The Budapest Convention (ETS No. 185) and its Protocols.** Budapest, 2001. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed on: May 20, 2024.
[232]EUROSTAT. **R&D expenditure**. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure&oldid=551418. Accessed on: May 31, 2024.
[233]EUROSTAT. **8% of EU enterprises used AI technologies in 2023.** May 29, 2024. Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240529-2. Accessed on: May 31, 2024.

claiming an important spot in such a relevant part of today's global economy.[234]

5.1 FEDERAL REPUBLIC OF GERMANY

The Federal Republic of Germany is a country in the western region of Central Europe, with a population of approximately 83.2 million people in 2024.[235] Germany became a ratified member of the United Nations Office on Drugs and Crime (UNODC) on 12 November 2014, having been a signatory nation since December 9, 2003.[236]

The **Deutsche Forschungsgemeinschaf***t* (DFG), also called German Research Foundation, is a self-governing funding organization and an association under private law in Germany, being a central figure in the German research field. Funding projects developed by the academic community, the DGF works with both sciences and humanities, promoting high-quality research at universities and non-university research institutions.[237]

With an annual budget of €3.9 billion provided by the German federal government and the states, the DFG funds research projects, creates competitions and conducts procedures for the evaluation of research proposals, shaping the conditions and standard of academic

[234]NINDL, Elisabeth. *et al*. **The 2023 EU Industrial R&D Investment Scoreboard.** Luxembourg: Publications Office of the European Union, 2023. Available at: https://dx.doi.org/10.2760/506189. Accessed on: May 27, 2024.
[235]WORLDOMETER. **Germany Population (2024).** Available at: https://www.worldometers.info/world-population/germany-population/. Accessed on: May 23, 2024.
[236]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles:** Germany**.** Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Fdeu.html. Accessed on: May 23, 2024.
[237]DFG - DEUTSCHE FORSCHUNGSGEMEINSCHAFT. **DFG, German Research Foundation.** Available at: https://www.dfg.de/en/dfg-profile/about-the-dfg/what-is-the-dfg. Accessed on: May 23, 2024.

research.[238] One of the institutions that are part of the DFG is the Max Planck *Gesellschaft* (Society), which is Germany's most successful research organization, with more than 15,000 yearly publications in renowned scientific journals.[239]

Another member is the Fraunhofer-Gesellschaft, a research organization prioritizing key future technologies and transferring its findings to industry in order to strengthen Germany as a center for industrial activity and for the benefit of society.[240] Other institutions linked to the DFG are the Helmholtz Association, Germany's largest scientific organization, composed of 18 scientific-technical and biological-medical research centers,[241] and Leibniz Association, which addresses social, economic, and ecological issues.[242]

Regarding the use of technologies like Artificial Intelligence (AI), Germany is working with partners in Europe in search of the balance between the opportunities and risks presented by AI. On the European Union's (EU) AI Act,[243] the German Economics Minister Robert Habeck says that the regulation's purpose is to take advantage of the potential of AI while being protected against the risks presented.[244]

Germany has been a ratified member of the Budapest Convention, also known as the Convention on Cybercrime, since 9

---

[238] *Ibidem.*

[239] MAX-PLANCK-GESELLSCHAFT. **Max Planck Society: Homepage.** Available at: https://www.mpg.de/short-portrait. Accessed on: May 23, 2024.

[240] FRAUNHOFER-GESELLSCHAFT. **Fraunhofer-Gesellschaft.** Available at: https://www.fraunhofer.de/en/about-fraunhofer.html. Accessed on: May 23, 2024.

[241] HELMHOLTZ-GEMEINSCHAFT DEUTSCHER FORSCHUNGSZENTREN. **Helmholtz Association.** Available at: https://www.helmholtz.de/en/about-us/. Accessed on: May 23, 2024.

[242] LEIBNIZ-GEMEINSCHAFT. **Leibniz Association.** Available at: https://www.leibniz-gemeinschaft.de/en/. Accessed on: May 23, 2024.

[243] DEUTSCHLAND.DE. **Rules for using artificial intelligence and Europe.** Available at: https://www.deutschland.de/en/topic/business/rules-for-using-artificial-intelligence-in-germany-and-europe. Accessed on May 23, 2024.

[244] EUROPEAN PARLIAMENT. **EU AI Act: first regulation on artificial intelligence | Topics**. Available at: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. Accessed on: May 23, 2024.

March 2003 with the Convention entering into force on 1 September 2009. The Convention is the first international treaty regarding crimes committed via the Internet and other computer networks, seeking to pursue a common criminal policy against cybercrime, harmonizing national laws, fostering international cooperation among nations, and improving the investigative techniques used when dealing with cybercrime.[245]

Furthermore, some of the offenses that are attended by the Budapest Convention are: computer-related fraud and forgery, illegal access, data interference, system interference, misuse of devices, offenses in child pornography, offenses in the infringements of copyrights and related rights. The offenses named in the convention are divided in 5 categories, with offenses against the confidentiality, integrity and availability of computer data and systems; computer-related offenses; content-related offenses; offenses related to infringement of copyright and related rights; and those offenses connected to ancillary liability and sanctions.[246]

There has been a recent rise in cyber attacks, specially from foreign agents, on German business, causing an estimated €148 billion in damage to the economy.[13] Given that, it is relevant to know which measures are used to counter this threat, such as the Cyber Security Strategy implanted by the German Federal Ministry of Internal Affairs in November 2016, which one of the objectives are the protection of critical information infrastructures, securing IT systems, the setting of a National

[245]COUNCIL OF EUROPE. **Budapest Convention - Cybercrime.** Available at: https://www.coe.int/en/web/conventions/full-list. Accessed on: May 23, 2024.
[246]COUNCIL OF EUROPE. **Convention on Cybercrime.** Budapest: Council of Europe, November 11, 2001. Available at: https://rm.coe.int/1680081561. Accessed on: May 23, 2023.

Cyber response Center that reports to the Federal Office for Information Security, and festive crime control in cyberspace.[247]

As a member of the European Union, Germany is a part of the Network and Information Security (NIS2) Directive, which obliges entities and sectors to take measures, increasing the cybersecurity in Europe in light of the surge in cyber-attacks.[248] Similarly, the EU also proposed the Cyber Resilience Act, which provides mandatory cybersecurity EU-wide, and the Digital Operational Resilience Act (DORA) focusing on the resilience of the financial sector against operational disruptions and cyber-attacks.[249]

According to the 2023 Global Organized Crime Index (OCINDEX) made by the Global Initiative Against Transnational Organized Crime (GI-TOC), the biggest criminal markets in Germany are: human trafficking; human smuggling; smuggling of weapons and other items; trade of ivory, pangolin scales and live animals; drug trading, especially cannabis, cocaine and amphetamines; cybercrimes.[250]

Furthermore, the occurrence of cybercrimes has increased in Germany, with the country having even declared a state emergency in the past years after a cyber-attack and the targeting of public administration by ransom or malware. These attacks have threatened

[247]EURONEWS. **Rise in cyber attacks on German business costing billions of Euros.** Euronews, May 13, 2024. Available at: https://www.euronews.com/business/2024/05/13/rise-in-cyber-attacks-on-german-business-costing-billions-of-euros. Accessed on: May 23, 2024.
[248]COUNCIL OF EUROPE. **Germany Cybercrime Community.** Available at: https://www.coe.int/en/web/octopus/-/germany. Accessed on: May 23, 2024.
[249]EUROPEAN PARLIAMENT. **The NIS2 Directive.** Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Accessed on May 23, 2024.
[250]GLOBAL INITIATIVE AGAINST ORGANIZED CRIME. **The Organized Crime Index**. Germany. Available at: https://ocindex.net/assets/downloads/2023/english/ocindex_profile_germany_2023.pdf.Accessed on: May 23, 2024.

many areas of German society and the risks of damage suffered by areas of critical infrastructure.[251]

Finally, Germany has domestic legislation regarding human trafficking, drugs, arms trafficking, and environmental crimes, with the federal criminal police having jurisdiction on the conducting of investigations related to the aforementioned trafficking. Also, the country is a signatory to all relevant treaties concerning organized crime.[252] [8]

Germany cooperates actively with both UNODC and the International Narcotics Control Board (INCB) in the enforcement of the Single Convention on Narcotic Drugs (1961), the Convention on Psychotropic Substances (1971), and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), with activities being coordinated by the Federal Ministry of Health and the Federal Government Drug Commissioner.[253]

On UNODC's Crime Programme, Germany has been one of the first signatories and a ratified member of the UN Convention on Transnational Organized Crime (UNTOC) and its Protocols, which cover trafficking in persons, smuggling of migrants, production and trafficking in firearms. The country is also a ratified member of the UN Convention against Corruption (UNCAC).[254]

Overall, Germany is one of the major donor countries between the members of UNODC, contributing to the general-purpose fund with money from the Foreign Office and the Ministry of Health, and to specific projects with funding from other ministries, such as the terrorism

---

[251] *Ibidem.*

[252] *Ibidem.*

[253] AUSWÄRTIGES AMT. **UNODC - United Nations Office on Drugs and Crime.** Available at: https://wien-io.diplo.de/iow-en/international-organizations/unodc/2001534. Accessed on: May 23, 2024.

[254] AUSWÄRTIGES AMT. **UNODC - United Nations Office on Drugs and Crime.** Available at: https://wien-io.diplo.de/iow-en/international-organizations/unodc/2001534. Accessed on: May 23, 2024.

prevention in Africa and police cooperation in Central Asia. Moreover, Germany has contributed to UNODC's Container Control Programme, focused towards reducing the trafficking of illegal goods, and co-chairs,[255] together with South-Africa, a group of friends of the Nelson Mandela Rules at the United Nations.[256]

5.2 REPUBLIC OF ESTONIA

The Republic of Estonia, located by the Baltic Sea, has established itself as a prominent player in the field of cybersecurity. Despite being a small country, with a population of just 1.3 million, it has emerged as a technological pioneer by evolving into a digital society since its independence from the Soviet Union in 1991.[257]

A study by the Inter-American Development Bank[258], which reviews advanced experiences in cybersecurity policies and practices, identifies Estonia as one of the leading countries with a dynamic approach focused on ensuring the provision of vital services and the interconnection of technology structures. This capability has made cybersecurity a hallmark of Estonian foreign policy, influencing not only the national security strategy but also the culture and mindset of its own

[255] *Ibidem.*

[256] UNITED NATIONS OFFICE ON DRUGS AND CRIME. **The United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules).** Available at: https://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf. Accessed on: May 23, 2024.

[257] ROBINSON, Nick; HARDY, Alex. Estonia: from the "Bronze Night" to cybersecurity pioneers. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 19, pp. 211-225.

[258] LEWIS, James Andrew. **Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States**. Inter-American Development Bank, 2016. Available at: https://publications.iadb.org/en/advanced-experiences-cybersecurity-policies-and-practices-overview-estonia-israel-south-korea-and. Accessed on: May 22, 2024.

society, thereby fostering advanced e-government services and a tech-savvy population.[259]

Nonetheless, Estonian cybersecurity hasn't always been as robust as it is today. In fact, the risks posed by data processing and management automation technology became evident when an interconnected system is developed without proper protection.[260] The great paradigm shifts for the country occurred after the Bronze Night on April 26, 2007, which triggered a series of cyber-attacks pointing at Estonian government systems for around three weeks.

The tensions began when the Bronze Soldier statue, a Soviet World War II memorial in central location, was relocated to the countryside, away from a prominent position. This action was strongly opposed by Estonia's Russian-speaking minority and the Russian government, resulting in violent street clashes that swiftly transitioned into the cybernetic framework.[261]

A targeted Distributed Denial-of-Service (DDoS) attack against the country obstructed government and civil society operations, flooding them with malicious traffic that temporarily disrupted state services and portals.[262] With the anonymity of the networks, these attackers were never properly identified, but they were a type of "hacktivists" with political motivation. This virtual offensive debilitated the nation's

[259] *Ibidem*.

[260] PRIISALU, Jaan; OTTIS, Rain. **Personal control of privacy and data: Estonian experience**. Health Technol, vol. 7, pp. 441-451, 2017. Available at: https://link.springer.com/article/10.1007/s12553-017-0195-1. Accessed on: May 22, 2024.

[261] ROBINSON, Nick; HARDY, Alex. Estonia: from the "Bronze Night" to cybersecurity pioneers. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 19, pp. 211-225.

[262] SALMA, Dita Aulia; MUNABARI, Fahlesa. **Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia**. Deviance Jurnal Kriminologi, vol. 7, pp. 32-45, Bekasi, Indonesia, 2023. Available at: https://journal.budiluhur.ac.id/index.php/deviance/article/view/2412. Accessed on: May 22, 2024.

information infrastructure, providing the world with a firsthand look at a significant cyber-attack.[263]

After this, concern about cybersecurity has afflicted political authorities across the European continent, and particularly the Estonian government. In 2008, the North Atlantic Treaty Organization (NATO) installed a Cooperative Cyber Defence Center of Excellence (CCDCoE), with the status of an international military organization, based in Tallinn, the capital of Estonia.

To avoid new cyber-attack complexes, the organization aims to support member nations "with unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy, operations and law".[264] In this sense, along with an independent international group of experts, it produced the "Tallinn Manual on the International Law Applicable to Cyber Warfare", an academic study and non-binding document focused on articulated extent legal norms to regulate the cybernetic field.[265]

These international efforts highlighted the pivotal shift that Estonia accomplished in cybersecurity, but it wasn't limited to that. Still in 2007, the country embarked on the development of a National Cyber Security Strategy aimed at mitigating the inherent vulnerabilities of cyberspace.[266] As part of this initiative, the Estonian Information Systems Authority (RIA)

---

[263]IASIELLO, Emilio. **Cyber Attack: A Dull Tool to Shape Foreign Policy**. Tallinn: NATO CCD COE Publications, 2013. Available at: https://www.ccdcoe.org/uploads/2018/10/24_d3r1s3_Iasiello.pdf. Accessed on: May 22, 2024.

[264]COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **About us: Our mission & vision**. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/about-us/. Accessed on: May 22, 2024.

[265]SCHMITT, Michael. **Tallinn Manual on the International Law Applicable to Cyber Warfare**: prepared by the International Group of Experts as the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

[266]ROBINSON, Nick; HARDY, Alex. Estonia: from the "Bronze Night" to cybersecurity pioneers. *In*: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 19, pp. 211-225.

gained more power, while the establishment of a Critical Information Infrastructure Protection Department (CIIP) sought to foster public-private collaboration.[267]

To reinforce defense procedures, in 2010, it was established the Estonian Defense League's Cyber Unit (KKL), made up of information technology specialists, dedicated to forming a sturdy public infrastructure capable of protecting the country during a cyber-attack.[268] In parallel, strategies were enhanced with the creation of the Cyber Security Council, serving as part of the Estonian government's Security Committee, which plays a crucial role in institutionalizing the country's response to cyber challenges.

Furthermore, the population was actively involved in this process. The government chose to be transparent about the attacks suffered, ensuring that citizens were aware of the threats and the measures being taken to protect cyberspace.[269] This approach allows them to be part of the securitization process for the country's digital systems and thus created a union of efforts that resulted in a highly informed society and tech-savvy nation.

As a result, these strategies strengthened Estonia's cybersecurity posture and served as a model for other countries to follow. After all, the Republic of Estonia transformed an adverse situation – from one of the

---

[267]SALMA, Dita Aulia; MUNABARI, Fahlesa. **Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia**. Deviance Jurnal Kriminologi, vol. 7, pp. 32-45, Bekasi, Indonesia, 2023. Available at: https://journal.budiluhur.ac.id/index.php/deviance/article/view/2412. Accessed on: May 22, 2024.

[268]JACKSON, Camille Marie. **Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success**. New Voices in Public Policy, vol. 7, 2013. Available at: https://www.semanticscholar.org/paper/Estonian-Cyber-Policy-After-the-2007-Attacks%3A-of-Jackson/ed3b6ecf3be6b14ee588f89ed95d501405a3c0c5. Accessed on: May 22, 2024.

[269]PRIISALU, Jaan; OTTIS, Rain. **Personal control of privacy and data: Estonian experience**. Health Technol, vol. 7, pp. 441-451, 2017. Available at: https://link.springer.com/article/10.1007/s12553-017-0195-1. Accessed on: May 22, 2024.

most significant cyberattacks ever experienced by a country – into a proactive and dynamic approach to cybersecurity.

Therefore, the country is at the forefront of global cyber defense initiatives, continually adapting to new threats and setting standards to protect information systems.

5.3 REPUBLIC OF SERBIA

The Republic of Serbia has been part of the United Nations Office on Drugs and Crime since 2003, having completed the ratification of its protocols in 2005.[270] Over the last years, the country, alongside most of its Balkans neighbors, has gone through a surge in cybercrime, specifically phishing and ransomware incidents. Research attributes this fact to inadequate public awareness and cybersecurity policies combined with a growing reliance on biometrics and digital identity in online banking, e-government services, and border control.[271]

Phishing[272] campaigns are one of the most common methods threatening the cybersecurity of the government and the financial sector. Many banks have alerted their customers about ongoing phishing and scam emails, with fraudsters creating fake social media accounts and organizing fraudulent giveaways. The public enterprise Post of Serbia was another frequent target of phishing campaigns. Scammers used

[270]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profile**: Serbia. 2024. Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Fsrb.html. Accessed on: May 27, 2024.

[271]ISPANOVIC, Igor, *et al*. **Battle for Balkan Cybersecurity**: Threats and Implications of Biometrics and Digital Identity. Balkan Insight, June 30, 2023. Available at: https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/. Accessed on: May 27, 2024.

[272]"Phishing" is the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Viber, other messaging apps, or email to falsely inform recipients that their packages were being held and required payment for release.[273]

Despite these incidents being reported, a recent report by the State Auditing Institution highlighted the need for improved communication between institutions and the National Computer Emergency Response Team. Public and governmental bodies and companies, afraid of negative press, often fail to report incidents to the authorities, resulting in some attacks remaining undetected for extended periods. This increases the risk and damage to the information infrastructure and data.[274]

Even though its effectiveness can be a matter of scrutiny, Serbia does have extensive legislation on cybercrime. Being a signatory of the Budapest Convention on Cybercrime, the country has mostly implemented its terms in their internal legislation, criminalizing online breaches, interference, fraud, child pornography and copyright infringement.[275] The International Telecommunication Union (ITU), however, classifies the legislation as obsolete when compared with the European Union, which greatly hinders the cooperation with the organism and even Serbia's candidacy into becoming a member State.[276]

With that in mind, the country has adopted several plans and strategies aimed at improving and harmonizing legislation of the Republic

---

[273]ISPANOVIC, Igor, *et al*. **Battle for Balkan Cybersecurity**: Threats and Implications of Biometrics and Digital Identity. Balkan Insight, June 30, 2023. Available at: https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/. Accessed on: May 27, 2024.
[274]ISPANOVIC, Igor, *et al*. **Battle for Balkan Cybersecurity**: Threats and Implications of Biometrics and Digital Identity. Balkan Insight, June 30, 2023. Available at: https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/. Accessed on: May 27, 2024.
[275]COUNCIL OF EUROPE. **Serbia**: Cybercrime legislation. Council of Europe, 2020. Available at: https://rm.coe.int/octocom-legal-profile-serbia-2020-updated-28may2020/. Accessed on: May 27, 2024.
[276]SANOU, Brahima; RELJIN, Irini. **Digital Innovation Profile**: Serbia. International Telecommunication Union, 2018. Available at: https://rm.coe.int/octocom-legal-profile-serbia-2020-updated-28may2020/. Accessed on: May 27, 2024.

with legal norms and standards of the European Union in the field of combating high-tech crime; improving organizational, personnel, technical and operational capacity of the state authorities competent for suppression of high-tech crime; improving preventive and proactive approach in the fight against high-tech crime; and improving cooperation at the national, regional and international level.[277]

All these actions show a notable effort to strengthen the national cybersecurity environment, as, in Serbia's case, it represents not only a matter of internal security, but a major aspect of its entry into the European Union.

5.4 REPUBLIC OF TÜRKYIE

The Republic of Türkyie changed its name in 2022, having it approved by the UN as a measure to broadly solidify the nation's cultural identity.[278] It has been in partnership with the United Nations Office on Drugs and Crime since its signing and approval of the United Nations Convention Against Corruption (UNCAC), officiated November 9, 2006.[279] Alongside corruption, narcotrafficking, transnational organized crime and now cybercrime are a part of the west-asian nation administration office.[280]

---

[277]COUNCIL OF EUROPE. **Serbia**: Cybercrime policies/strategies. Council of Europe, 2020. Available at: https://www.coe.int/en/web/octopus/-/serbia. Accessed on: May 27, 2024.
[278]THE GUARDIAN. **Turkey officially changes name at UN to Türkiye.** Available at: https://www.theguardian.com/world/2022/jun/03/turkey-changes-name-to-turkiye-as-other-name-is-for-the-birds. Accessed on: May 25, 2024.
[279]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification Status.** Available at: https://www.unodc.org/unodc/en/corruption/ratification-status.html. Accessed on: May 25, 2024.
[280]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Statement of the Republic of Turkey.** Available at: https://www.unodc.org/documents/commissions/CND/CND_Sessions/CND_63/Statements63_02.03.2020/Country_02.03.2020/Turkey.pdf. Accessed on: May 25, 2024.

The country is also at a defender position for open technological communication around the world by joining the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.[281] The Turkish government was part of the International Classification of Crime for Statistical Purposes (ICCS) and the creation of the Technical Advisory Group as a policy to not only improve crime identification but solutional operations.[282]

Although reprimanding non-governmental organizations (NGOs) and private stakeholders for active participation in the convention because of disregarding commanding principles, the country understands the need to include cooperative counseling.[283] A few of the intended adopted tactics proposed by representatives included leveraging threat intelligence, risk assessment, safe use of new generation technologies (5G, AI, IoT) and better definition of informational criminal matters and enlarging resource acquisition between States.[284]

Their cybercrime combating mission started as early as a decade ago. The International Cyber 2014 Exercise was conducted amongst 19 countries with the help of the Ministry of Transport, Maritime Affairs and Communication alongside the Information Technologies and Communications Authority (ICTA) and International Telecommunication

---

[281]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Turkey's Initial Views regarding the Scope, Objectives and Structure of an International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Turkey_-_AHC_Initial_Views.pdf. Accessed on: May 25, 2024.

[282]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Report of the United Nations Office on Drugs and Crime on the International Classification of Crime for Statistical Purposes.** Available at: https://unstats.un.org/unsd/statcom/doc15/Intervention-3c-Turkey.pdf. Accessed on: May 25, 2024.

[283]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **1st Statement - Turkish Mission to the UN.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Session_org_matters/Turkey.pdf. Accessed on: May 25, 2024.

[284]*Ibidem.*

Union (ITU) to increase awareness, information access contributions within State cooperation commissions.[285]

Despite all efforts, institutional digitization processes and the consumption of Internet of Things (IoT) tools have led the country to be the most targeted region in the year of 2023.[286] Industrial Control Systems (ICS) computers were a lucrative mean for phishing and infrastructure attacks as the manufacturing of various daily life aspects such as automation, cars, energy, mining, and monetary transactions are made on them.[287]

Internal tech crimson vigilant parties account for structure with the 2013 Department for Cybercrime and the National Cyber Security Strategy and Action Plan 2020-2023 overseen by the National Cyber Security Board and USOM, a nationally spread center for emergency responses, which covers public and private all-size industries and legal-persons, including top defense companies in the country: Aselsan and Havelsan, systemic cyberattack fighters and STM, for cybersecurity support offered through their CyDecSys program.[288]

Aiming for protection and the enhancement of home capacity, strength, security network and international assistance when demanded, legislation includes specific provisions related to cybercrime were included in its Penal Code punitive actions for crimes such as network illegal accessing, alteration, deleting, corruption of data and banking

---

[285]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Cybercrime reporting and prevention.** Available at: https://sherloc.unodc.org/cld/lessons-learned/tur/cybercrime_reporting_and_prevention.html?. Accessed on: May 25, 2024.

[286]DAILY SABBAH. **Türkiye becomes world's most cyber targeted region in 2023.** Available at: https://www.dailysabah.com/turkiye/turkiye-becomes-worlds-most-cyber-targeted-region-in-2023/news. Accessed on: May 25, 2024.

[287]*Ibidem.*

[288]AA ENERGY. **Turkey fights cyber crimes with own capabilities.** Available at: https://www.aa.com.tr/en/energy/energy-projects/turkey-fights-cyber-crimes-with-own-capabilities/23772. Accessed on: March 26, 2024.

information, online gambling, counterfeiting of documents obscenity, larceny by the use of data and even communication fraud.[289]

To complete recent policy-making strategies and complement government equipping, the Security Board has regulated internet broadcasting and cautious development and promotion of new generation technologies. Additionally, a Personal Data Protection Board and the National Artificial Intelligence Strategy were provided in hope that the nation is included in a list for top 20 countries for AI.[290]

The National Artificial Intelligence Strategy Steering Committee plans stand for educational campaigns in AI for increasing employment and the launching of at least one global initiative and operating spin-offs coming from research support.[291] Public incentives for entrepreneurship and innovation companies were also set, they are expected to dive into quality data and base framework to quicken economical adjustments GDP endowments up to five percent by 2025.[292]

5.5 RUSSIAN FEDERATION

The legal former Union of Soviet Socialist Republics (USSR)'s successor has always had a place of renown in the history of cybernetic security and advancements. The Russian Federation has been a protagonist in several international cyber related events, such as

[289]COUNCIL OF EUROPE. **Turkey Status regarding Budapest Convention.** Available at: https://www.coe.int/en/web/octopus/-/turkey. Accessed on: May 26, 2024.
[290]AI BUSINESS. **Turkey publishes its National Artificial Intelligence Strategy.** Available at: https://aibusiness.com/verticals/turkey-publishes-its-national-artificial-intelligence-strategy. Accessed on: May 26, 2024.
[291]AI BUSINESS. **Turkey publishes its National Artificial Intelligence Strategy.** Available at: https://aibusiness.com/verticals/turkey-publishes-its-national-artificial-intelligence-strategy. Accessed on: May 26, 2024.
[292]DIGITAL TRANSFORMATION OFFICE. **National Artificial Intelligence Strategy 2021-2025.** Available at: https://cbddo.gov.tr/en/. Accessed on: May 26, 2024.

accusations of espionage[293] and the race for the development of new technologies during the Cold War.[294] Nevertheless, Soviet softwares and technologies have also, indirectly, made the USSR - and its subsequent successor states a significant part in the conversation regarding cybercrimes and related activities internationally.

The Russian Federation joined UNODC on December 9th, 2003, and underwent ratification on May 9th, 2006. Thus, after officially joining the Office, began their joint endeavors in the subject of cybersecurity and jurisdiction on the internet. It is also important to note that the USSR's delegation was already involved with the resolution of such matters - on an international scale - in the form of collaboration with international governments at the United Nations (UN).

Being that as it may, since 1984, long before the creation of the committee as it is today, as the successor of the Soviet Union's permanent member seat, the Russian Federation automatically assumed its place in the security council in the UN after the dissolution of 1991.[295]

When it comes to the development of actual R&D technologies, Russia has been heavily investing in this area, with a substantial amount of growth to show for it, managing to rank 42º among the leading digital economies in the world, according to the International Monetary Fund (IMF).[296] Although there aren't any specific projects on the development

---

[293]MATLACK, Carol. **"The Company Securing Your Internet Has Close Ties to Russian Spies"**. Germany: Bloomberg.com. Archived from the original on 2015-03-20. Available at: https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies. Accessed on: May 20, 2024.

[294]GRAHAM, Loren R.(2004) **Science in Russia and the Soviet Union. A Short History.** Series: Cambridge Studies in the History of Science. Cambridge: Cambridge University Press, February 26, 1993. ISBN 978-0-521-28789-0

[295]BLUM, Yehuda Z. **Russia Takes Over the Soviet Union's Seat at the United Nations**. Oxford: European Journal of International Law, Oxford University Press, August 2, 1999. Archived from the original on March 12, 2005. Available at: https://web.archive.org/web/20050312051908/http://www.ejil.org/journal/Vol3/No2/art8-02.html#TopOfPage. Accessed on: May 20, 2024.

[296]INTERNATIONAL MONETARY FUND. **World Economic Database.** Available at: https://www.imf.org/en/Publications/WEO/weo-database/2022/April (2022). Accessed on: May 20, 2024.

of such tech funded only by the government, there are private companies located in Russia with significant contributions in this regard. One such business would be Kaspersky Lab[297], specialized in the development of antivirus and cybersecurity related technology, also recognized globally by its achievements in this area of expertise.[298]

With reference to internal legislation in relation to cybercrimes, the Russian Federation has been hammering down a significant number of domestic criminals since the beginning of 2022, utilizing a multidirectional approach to the issue at hand, by having different administrative entities working on the same matter, all at once.[299]

Starting with the Federal Security Service (FSB), who reports directly to the federal administration, whose main responsibilities are overseeing Russian national security, counter-terrorism, border protection, information security, and counterintelligence. Not only that, but also the protection of territorial waters, which constitutes Russia's exclusive economic zone, and its natural resources.[300]

The FSB is primarily a domestic security agency. However, in recent years it has gradually increased its influence over Russia's internal politics, mainly through its competencies to investigate white-collar crimes.[301] Although the agency's focus is primarily domestic, it is

---

[297]KASPERSKY LAB. **About.** Moscow: Kaspersky. Available at: https://usa.kaspersky.com/about. Accessed on: May 20, 2024.

[298]STATISTA RESEARCH DEPARTMENT. **Worldwide Endpoint Security Revenue by Vendor, 2010**. Statista, September 2021. Available at: https://www.statista.com/statistics/461754/share-of-gdp-expenditure-on-research-and-development-russia/. Accessed on: May 21, 2024.

[299]FLASHPOINT INTEL TEAM. **Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way.** Washington, DC: *FLASHPOINT.com*. Washington, DC. Available at: https://flashpoint.io/blog/russian-cybercrime-law-enforcement-bodies-fsb-mvd-deptk/. Accessed on: May 19, 2024.

[300]RUSSIAN FEDERATION. **Russian Federation Federal Law No. 40-FZ. Adopted by the State Duma 22 February 1995**. Archived 16 August 2018 at the Wayback Machine.. Available at: https://www.consultant.ru/document/cons_doc_LAW_6300/. Accessed on: May 21, 2024.

[301]SCHNEIDER, Eberhard. **The Russian Federal Security Service under President Putin.** In: White, S. (eds) Politics and the Ruling Group in Putin's Russia. Studies in Central and Eastern Europe. Palgrave Macmillan, London. https://doi.org/10.1057/9780230583061_3. Accessed on: May 21, 2024.

occasionally also active beyond Russia's borders. Beyond its internal predilection, the FSB specializes in countering foreign interference in internal affairs and preventing activity that could undermine any area of the state's defense capabilities.[302] These blurred lines have led to accusations of international cyberattacks and assassinations carried out by the FSB.[303/304/305]

Other than what has already been discussed, there is also the Ministry of Internal Affairs (MVD)[306], which is the federal executive authority of the Russian Federation. Headed by a minister appointed by the president of Russia, the MVD oversees internal troops and the police, whose tasks are to maintain law and order and suppress offenses on the national territory.[307]

The formation is primarily responsible for crime prevention, drug control and migration affairs. It is a paramilitary organization that has the right to acquire military small arms for its personnel. The activities of MVD are regulated by the Code of Criminal Procedure of the Russian Federation.[308]

---

[302]*Ibidem.*

[303]REUTHERS, Thomson. **Russia responsible for killing of Alexander Litvinenko, European rights court rules.** Published by CBC News, 2021. Available at: https://www.cbc.ca/news/world/russia-litvinenko-echr-1.6183645. Accessed on: May 20, 2024.

[304]LITVINENKO, Alexander; FELSHTINSKY, Yuri. **Blowing up Russia: terror from within.** Vol 1. Rússia: S.P.I. Books, 2002.

[305]COCKBURN, Patrick. **Boris Kagarlitsky, a member of the Russian Academy of Sciences Institute of Comparative Politics, writing in the weekly Novaya Gazeta, says that the bombings in Moscow and elsewhere were arranged by the GRU**. Independent.co.uk. Archived from the original on 27 August 2009. Available at: https://web.archive.org/web/20090827150331/https://www.independent.co.uk/news/world/europe/russia-planned-chechen-war-before-bombings-727324.html. Accessed on: May 21,2024.

[306]WELT, Cory; NELSON, Rebecca N. **Russia: domestic politics and economy 9, 2021.** Published September 9,2021. CRS Report No. R46518. Available at: https://crsreports.congress.gov/product/pdf/R/R46518. Accessed on: May 19, 2024.

[307]*Ibidem.*

[308]VYTOVTOV, A.E. **Revisiting the Concept of Economic Crimes in Russian Criminal Legislation**. Gaps in Russian Legislation, v.16, n4, p.374-378, august 2023. ISSN 2072-3164 (Print) ISSN 2310-7049 (Electronic).

Under the MVD, there's also a specialized division that has been active since 2001, named Departament K - short for **Компьютерные преступления** (**Kompyuternye Prestupleniya**), or computer crimes - who focuses mainly on information technology related crimes, which later evolved into our current notions on what constitutes cybercrime.[309] In addition, according to the official information on the MVD website[310], the department is responsible for addressing crimes such as: unlawful access to legally protected information, creation, use, and distribution of malicious programs, violation of the rules for the operation of storage media, information technology-related fraud, production and distribution of pornographic content directed against minors and illegal use of objects of copyright.[311]

When it comes to Russia's involvement against cybercrime, the selling of drugs and similar illicit activities, it is important to take into account the delegation's participation with UNODC.[312] In 2021, from September 13 to 17, The Regional Programme for Afghanistan and Neighboring Countries supported an online training course for middle-level officers that was conducted by the UNODC Programme Office in Turkmenistan.[313] Additionally, The 4 day training was organized by the Siberian Law Institute of the MVD and within the framework of the

[309]FLASHPOINT INTEL TEAM. **Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way.** Washington, DC: FLASHPOINT.com. Available at: https://flashpoint.io/blog/russian-cybercrime-law-enforcement-bodies-fsb-mvd-deptk/. Accessed on: May 19, 2024.

[310]RUSSIA. Ministry of internal affairs of the Russian Federation. Acting minister status. Available at: http://government.ru/en/department/86/events/. Accessed on: May 20, 2024.

[311] Ibidem.

[312]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC-Russia Partnership on Counter-Narcotics Training for Central Asia, Afghanistan and Pakistan (Phase IV)**. September 13-17, 2021. Available at: https://www.unodc.org/rpanc/en/Sub-programme-1/unodc-russia-partnership-on-counter-narcotics-training-for-central-asia--afghanistan-and-pakistan-phase-iv.html. Accessed on: May 20, 2024.

[313]*Ibidem.*

UNODC-Russia Partnership on Counter-Narcotics Training for Central Asia, Afghanistan and Pakistan.[314]

For a better understanding of their measures, the entire discussion surrounding this nation's involvement with international affairs needs to be analyzed through the lens of their understanding towards the internet and boundaries. As is with any country, the Russian federation has its own perception and ideals concerning cybercrimes, international boundaries on the internet and the availability of data, and it differs significantly compared to most of the western hemisphere.[315]

In particular, Russia has deep concerns over the presumption that national borders are of minor relevance in this matter and on the principle of uncontrolled exchange of information in cyberspace. More specifically, the circulation of information which may pose a threat to society or the state, and sovereignty of the “national internet”, is a key security concern in Russia, but mostly not recognized as such in the West.[316]

> Dialogue between Russia and Western partners on cyberspace issues is hampered not only by a difference in understanding of specific concepts, but also in fundamental assumptions and in norms which are taken for granted by one side but seen as threatening by the other. One such assumption

[314] *Ibidem*.

[315] GILES, Keir. Russia and cyber security. *In:* **Nação e Defesa.** 2012, n.º 133, 5.ª ed. p. 69-88. Available at: https://comum.rcaap.pt/bitstream/10400.26/42460/1/Giles_Keir_Russia%20and%20cyber%20security_NeD133_p_69_88.pdf. Accessed on, May 19, 2024.

[316] *Ibidem.*

> regards the free circulation of information on the internet.[317]

In relation to that, their measures for combating cybercrime may also revolve around advocating for the limitation of free range data navigation, the establishing of national perimeters for online spaces and the enforcing of national sovereignty over matters that partake in the interweb.[318] In that way, Russia hopes to raise national control over the unlimited circulation of data-related crimes and prevent sensitive information from being exposed to the detriment of their government.[319]

In conclusion, the Russian Federation has a long history of participating, together with outside collaboration, in the war against drugs and crime. Not only that, but also regarding international involvement in matters of technological advancements and the development of new technologies. For that reason, this nation holds an important and irreplaceable spot in the discussion partook at UNODC, and it also may be one of the main contributors to resolving problems related to drug and crime prevention in cyberspace globally.

5.6 UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

[317]GILES, Keir. Russia and cyber security. *In:* **Nação e Defesa.** 2012, n.º 133, 5.ª ed. p. 69-88. Available at: https://comum.rcaap.pt/bitstream/10400.26/42460/1/Giles_Keir_Russia%20and%20cyber%20security_NeD133_p_69_88.pdf. Accessed on, May 19, 2024.
[318]*Ibidem.*
[319]*Ibidem.*

The United Kingdom of Great Britain and Northern Ireland (UK) is an island nation located north-west of mainland Europe,[320]with a population of roughly 67.9 million people.[321/322] A founding member of the United Nations (UN) on 24 October 1945,[323] the United Kingdom of Great Britain and Northern Ireland became a signatory of the United Nations Office on Drugs and Crime (UNODC) on 9 December 2003, becoming a ratified member on 9 February 2006.[324]

Two of the world's most prestigious universities, the University of Cambridge and the University of Oxford, are located in the United Kingdom. Both renowned for their research fields and have constant collaborations between academics. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", a report made by the former Oxford University's Future of Humanity Institute (FHI) and the Centre for the Study of Existential Risk (CSER) from Cambridge, with others collaborators, focuses on malicious Research and Development (R&D) in Artificial Intelligence (AI), analyzing the risks presented by this form of R&D and trying to create a defense system against them.[325]

In the aforementioned report, several recommendations were made regarding protecting against AI systems risks whilst being able to use the beneficial applications, such as the close collaboration between

---

[320]THE COMMONWEALTH. **United Kingdom.** Available at: https://thecommonwealth.org/our-member-countries/united-kingdom. Accessed on: May 21, 2024.
[321]WORLDOMETER. **U.K. Population (2024).** Available at: https://www.worldometers.info/world-population/uk-population/#google_vignette. Accessed on: May 21, 2024.
[322]WORLD POPULATION REVIEW. **London Population 2024.** Available at: https://worldpopulationreview.com/world-cities/london-population. Accessed on: May 21, 2024.
[323]UNITED NATIONS. **History of the United Nations.** Available at: https://www.un.org/en/about-us/history-of-the-un. Accessed on May 21, 2024.
[324]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles: United Kingdom of Great Britain and Northern Ireland.** Available at: https://www.unodc.org/unodc/en/corruption/country-profile/countryprofile.html#?CountryProfileDetails=%2Funodc%2Fcorruption%2Fcountry-profile%2Fprofiles%2Fgbr.html. Accessed on: May 21, 2024.
[325]BRUNDAGE, Miles, et al.**The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation.** Future of Humanity Institute, et al. February, 2018. Available at: https://arxiv.org/pdf/1802.07228.pdf. Accessed on: May 21, 2024.

policymakers and technical researchers to investigate, prevent, and mitigate the potential malicious use of AI.[326] On 2018, the UK Government released a National AI Strategy[327] with plans to ensure that the beneficial aspects of AI systems would be available to all sectors and regions, working with partners such as The Alan Turing Institute on the safety and ethics side of it, with the institute releasing a guide on the subject.[328]

Furthermore, the UK Research and Innovation (UKRI) is the United Kingdom's national funding agency sponsored by the Department for Science, Innovation and research Technology (DSIT),[329] launched in April 2018 and investing in research and science in the country.[330] Scattered across different areas to deliver societal, economic, and scientific benefits beyond the UK, the UKRI's institutes are formed by research and innovation organizations, such as research and technologies organizations (RTOs), the Catapults[331] (technologies and innovation centers), public sector research establishments, independent research organizations (IROs), and specialist higher education providers like the Institute for Cancer Research.[332]

---

[326] *Ibidem.*

[327] HM GOVERNMENT. **National AI Strategy.** Available at: https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf. Accessed on: May 21, 2024.

[328] THE ALAN TURING INSTITUTE. **Understanding artificial intelligence ethics and safety.** Available at: https://www.turing.ac.uk/sites/default/files/2019-08/understanding_artificial_intelligence_ethics_and_safety.pdf. Accessed on: May 21, 2024.

[329] UNITED KINGDOM. **UK Research and Development.** Available at: https://www.gov.uk/government/organisations/uk-research-and-innovation. Accessed on: May 21, 2024.

[330] UK RESEARCH AND DEVELOPMENT. **About UK Research and Innovation.** Available at: https://www.ukri.org/who-we-are/about-uk-research-and-innovation/. Accessed on: May 21, 2024.

[331] The Catapults are a network of centers set up by Innovate UK in the United Kingdom, to promote research and development (R&D), productivity and economic growth.

[332] UK RESEARCH AND DEVELOPMENT. **Explainer: how UKRI's institutes support research and innovation.** Available at: https://www.ukri.org/publications/explainer-ukris-institutes/explainer-how-ukris-institutes-support-research-and-innovation/. Accessed on: May 21, 2024.

The UKRI provides core funding to more than 60 institutes and catapults in the UK, those being extremely varied in their purpose, governance, and disciplinary and sector focus. The funding supports long-term capability within institutes by supplying expertise, knowledge and equipment to fulfill their respective goals. Regarding how they are governed, the institutes are divided in those which are wholly owned by UKRI thus being part of the public sector, the legally-independent institutes, and the embedded ones which are fully hosted by another organization, generally a university.[333]

Furthermore, a significant part of UKRI's budget is headed towards the institutes and catapults, nearly amounting to £1.5 billion in 2020 to 2021, with the funding going through three main channels: core capability funding, capital from World Class Laboratories Fund and other major capital investments and upgrades, and competitive grants won from across UKRI.[334]

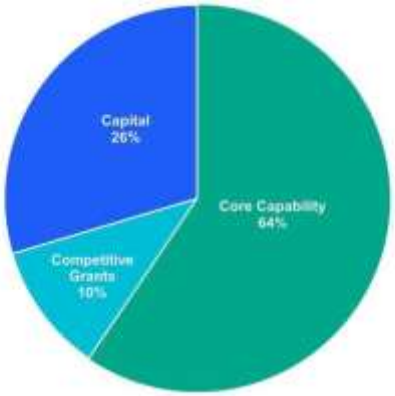
Some of the institutes also receive funding from external sources, such as government departments, charities and business, philanthropic donations, commercial income, and international sources of funding including Horizon programmes - which are a part of Horizon Europe, the European Union's (EU) funding programme for research and innovation.[335]

Image 08: Three main channels funded by UKRI.

[333] *Ibidem.*

[334] *Ibidem.*

[335] EUROPEAN COMMISSION. **Horizon Europe.** Available at: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en. Accessed on: May 21, 2024.

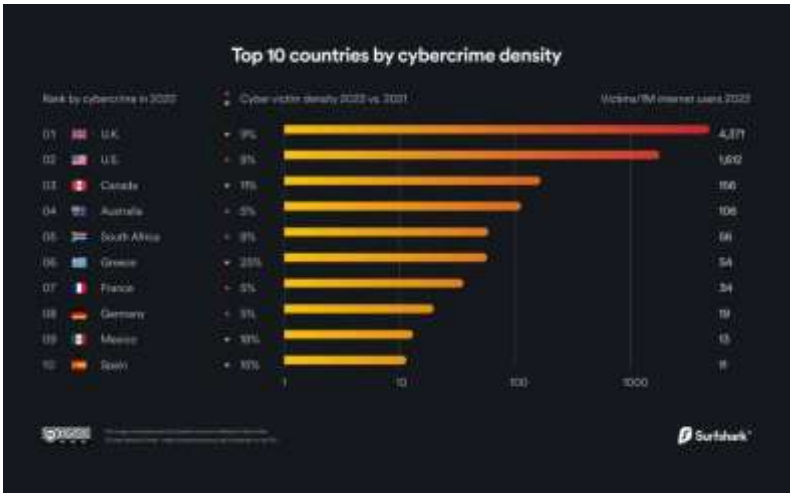


Source: UK Research and Development.[336]

Also, on 4 March 2024, the Chancellor of the Exchequer Jeremy Hunt announced an investment of £360 million in the UK's R&D and manufacturing projects as a part of the government's plan in economic growth, improvement on health resilience and to support jobs. Considering that a lot of the risks presented by new technologies during recent times are involved with cyberspace, it is relevant to mention that by 2022, the United Kingdom led the cybercrime density list with 4,371 victims per 1M internet users.[337]

Image 09: Top 10 countries by cybercrime density.

[336]UK RESEARCH AND DEVELOPMENT. **Explainer: how UKRI's institutes support research and innovation.** Available at: https://www.ukri.org/publications/explainer-ukris-institutes/explainer-how-ukris-institutes-support-research-and-innovation/. Accessed on: May 21, 2024.
[337]UNITED KINGDOM. **£360 million to boost British manufacturing and R&D.** Available at: https://www.gov.uk/government/news/360-million-to-boost-british-manufacturing-and-rd. Accessed on May 21, 2024.



Source: Surfshark.[338]

The Computer Misuse Act 1990 (CMA),[339] which is the main legislation relating to offenses or attacks against computer systems in the United Kingdom, criminalizing unauthorized access to computer systems and data, and the damaging and destroying of these. However, due to the time passed since the creation of the CMA, and to ensure the UK's legislative framework continues to support action against crimes occurring online, the Government decided to conduct a review of the Act.[340]

After receiving responses from stakeholders over what could be done against criminals, being some of the responses related to online harms such as deep fake imagery, whether new technologies like AI systems are adequately covered under the CMA, and offense of

[338]SURFSHARK. **Cybercrime statistics.** Available at: https://surfshark.com/research/data-breach-impact/statistics. Accessed on: May 21, 2024.
[339]THE CROWN PROSECUTION SERVICE. **Cybercrime - prosecution guidance.** Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Accessed on: May 21, 2024.
[340]UNITED KINGDOM. **Review of the Computer Misuse Act 1990: consultation and response to call for information.** Available at: : https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible. Accessed on: May 21, 2024.

possession of illegally obtained data, the Government gathered proposals for legislative change.[341]

One of the aforementioned proposals was domain name and IP address takedown and seizure, seeing that the use of domain names and IP addresses in support of criminality has caused considerable damage to the population, with the limitations that law enforcement agencies would need to apply to a court for the order, demonstrating evidence to support requirements.

Another proposal is the power to preserve data, with the creation of a power enabling law enforcement agencies to request the preservation of specific computer data by its owner to prevent it from being deleted.[342] Finally, the last proposal presented relates to data copying, with the Government considering the need for the creation of a general offense for possessing or using illegally obtained information.[343]

In addition, the Cyber Protect is a network that exists across the UK and provides free cyber awareness training to organizations, such as public services, local government, business, and education.[344] Being part of the UK Cyber Protect network, the Police Services of Northern Ireland's Cube Crime Centre, aims to improve the defense of small and medium-sized enterprises (SMEs), charity and organizations against cyber attacks.[345] The Cyber Crime Centre also promotes the services offered by the National Cyber Security Centre (NCSC), which acts as a

[341] *Ibidem.*
[342] *Ibidem.*
[343] *Ibidem.*
[344] REGIONAL ORGANISED CRIME UNIT. **Cyber Protect.** Available at: https://southeastcyber.police.uk/protect/. Accessed on: May 21, 2024.
[345] POLICE SERVICE OF NORTHERN IRELAND. **Cyber Protect.** Available at: https://www.psni.police.uk/safety-and-support/online-safety/cyber-protect. Accessed on: May 21, 2024.

bridge between industry and government, providing support on cyber security.[346]

Furthermore, the Budapest Convention, also known as the Convention on Cybercrime, is the first international treaty regarding crimes committed via the Internet and other computer networks, dealing with violations of network security, infringements of copyright, computer-related frauds, and child pornography.[347] With the purpose to pursue a common criminal policy aimed at the protection of society against cybercrime, the legislative framework allows practitioners from Parties to cooperate internationally. The Convention came into force for the United Kingdom on 1 September 2011.[348]

With the continuous digital transformation in the world, the Internet has been used maliciously by those involved in the trafficking of humans, drugs, and other illicit materials. The United Kingdom has worked extensively with UNODC with the 2022 edition of the Global Report on Trafficking in Persons (GLOTIP),[349] recalling that the UN Protocol to Prevent, Suppress and Punish Trafficking In Persons, Especially Women and Children has been ratified in the United Kingdom since 2006, which intends to prevent and combat crimes of this type, facilitating international cooperation against it.[350] Also, the UK has funding

---

[346]UNITED KINGDOM. **National Cyber Security Centre.** Available at: https://www.gov.uk/government/organisations/national-cyber-security-centre. Accessed on: May 21, 2024.
[347]COUNCIL OF EUROPE. **The Budapest Convention.** Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed on: May 21, 2024.
[348]UNITED KINGDOM. **Convention on cybercrime.** Available at: https://www.gov.uk/government/publications/convention-on-cybercrime--2. Accessed on: May 21, 2024.
[349]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Global Report on Trafficking in Persons 2022.** Available at: https://www.unodc.org/documents/data-and-analysis/glotip/2022/Western_and_Southern_Europe.pdf. Accessed on: May 21, 2024.
[350]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.** New York: November 15, 2000. Available at: https://www.unodc.org/documents/treaties/Special/2000_Protocol_to_Prevent_2C_Suppress_and_Punish_Trafficking_in_Persons.pdf. Accessed on: May 21, 2024.

agreements in support of UNODC's anti-corruption activities, further adding the implementation of the UN's Convention Against Corruption.[351]

On the UN Cybercrime Treaty, some of the things cited in the United Kingdom National Submission are: the focus of the new international convention should be strengthening cooperation against criminal activity; the UN Treaty should cover both cyber-dependent offenses and cyber-enabled crimes, in which the scale of the offense is increased by the use of the cyberspace; the development of the Treaty being made in an inclusive and transparent manner, with the treaty's provision encouraging the same approach to tackling cybercrime.[352]

Finally, the UK believes that the purpose of the treaty should be to support the cooperation of national law enforcement and prosecutorial agencies, bilaterally or multilaterally, in the investigation and prosecution of the offenses set out in the treaty.[353]

5.7 UKRAINE

The World Cybercrime Index (WCI) – which considers the overall amount of cybercrimes, the impact of such crimes and the professionalism and technical skill of the offenders in order to determine which countries house the biggest cybercrime threats – ranks Ukraine as

[351]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UK announces new financial contributions to support UNODC's anti-corruption work**. Available at: https://www.unodc.org/unodc/en/frontpage/2018/December/uk-announces-new-financial-contributions-to-support-unodcs-anti-corruption-work.html?ref=fs1. Accessed on: May 21, 2024.
[352]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UK National Submission on the UN Cybercrime Treaty.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/UK_AHC_National_Statement.pdf. Accessed on: May 21, 2024.
[353]*Ibidem.*

the world's second biggest cybercrime hotspot, shortly behind Russia.[354] The country of Ukraine is no stranger to cyber-attacks, its familiarity with them dating back to the Russian annexation of Crimea, in 2014; since then, the country has endured cyber-attacks on the Ukrainian election system in 2014, energy blackouts in 2015, and the Petya ransomware attack in 2017.[355]

Consequently, Ukraine has had a decade-long experience fending off cyber-attacks, the likes of which became more frequent from mid-2021 on and peaked around Russia's full-scale invasion. The Security Service of Ukraine (SSU) has units specialized in building up defenses against these kinds of threats, and claims that the Ukrainian Cyber Security Situation Centre has "detected and neutralized almost 10,000 cyberattacks and cyber incidents" ever since the beginning of the war.[356]

This experience has shaped the country into a kind of laboratory for cutting-edge cyber weapons, with Ukraine's military intelligence agency launching cyberattacks of their own, such as the barrage of distributed denial-of-service (DDoS) attacks against United Russia's (Russia's ruling party's) servers, websites, and domains in April 2024.[357]

The series of high-profile cyber operations conducted at the beginning of the Russo-Ukrainian war led many to believe it to be the world's first genuine "cyber war". However, Microsoft observed that over 50% of destructive Russian cyber-attacks occurred in the first 6 weeks of

---

[354]BRUCE M., LUSTHAUS J., KASHYAP R., PHAIR N, VARESE F. **Mapping the global geography of cybercrime with the World Cybercrime Index**. PLoS ONE 19(4): e0297312. Available at: https://doi.org/10.1371/journal.pone.0297312. Accessed on: May 27, 2024.

[355]YANKOVSKI, A. **Key lessons from Ukraine's eight-year struggle against russian cyber warfare - KPMG Ukraine**. Available at: https://kpmg.com/ua/en/home/media/press-releases/2022/11/key-lessons-from-ukraines-eight-year-struggle-against-russian-cyber-warfare.html. Accessed on: May 27, 2024.

[356]SECURITY SERVICE OF UKRAINE. **Cyber Security Situation Centre**. Available at: https://ssu.gov.ua/en/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky. Accessed on: May 27, 2024.

[357]CSIS. **Significant Cyber Incidents | Center for Strategic and International Studies**. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed on: May 27, 2024.

the conflict – generally in tandem with kinetic military actions[358]–, and many experts maintain that, 2 years later, such operations have had a limited impact on the fighting and are instead mainly used as tools for intelligence-gathering and influencing.[359]

That is not to say, although that large-scale cyber operations are no longer a threat, especially so in times of war. In December of 2023, the Ukrainian telecommunications giant Kyivstar, estimated to have at least 24 million mobile customers and a million home internet users, was targeted in what has been popularly regarded as a "powerful hacker attack", where users were left with no phone or internet access and air-raid sirens malfunctioned as a result of the outage.[360]

During its investigation of the incident, the SSU assessed that the hackers had attempted to penetrate Kyivstar earlier that year, and after obtaining full access to its servers in November, they would have been able to steal personal information and Telegram accounts from the users, trace the locations of phones and intercept SMS messages.[361]

In this setting, the International Humanitarian Law (IHL) also comes into play, for there is uncertainty regarding how the law applies when considering cyber operations crossing a threshold at which they are considered an act of war: the prominent role of non-governmental actors such as private companies and civilian hackers blurs the line of

[358]MATAMIS, J. **False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War • Stimson Center**. Available at: https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/. Accessed on: May 27, 2024.
[359]*Ibidem.*
[360]PARKER, J. **Ukraine mobile network Kyivstar hit by "cyber-attack"**. BBC News, December 12, 2023. Available at: https://www.bbc.com/news/world-europe-67691222. Accessed on: May 27, 2024.
[361]BALMFORTH, T. **Exclusive: Russian hackers were inside Ukraine telecoms giant for months.** Reuters, January 5, 2024. Available at: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/. Accessed on: May 27, 2024.

who is a combatant and who is a civilian, and therefore of who is protected under the IHL.[362]

In the Ukrainian Dark Web, an increasing number of hacker alliances supportive of the country have been forming – some, such as the Ukrainian Hacker Alliance, having existed since 2016[363] – as it appears that many hackers of the world are favoring Ukraine instead of Russia: the famous hacker collective Anonymous, for example, hacked a Russian live TV broadcast in order to put up the message "ordinary Ukrainians are against the war" in 2022.[364] Furthermore, the Deputy Prime-Minister and Minister of Digital Transformation of Ukraine announced on social media that the country was attempting to create the "IT Army of Ukraine" and thus looking for digital talents. The army is said to be about 400,000 people strong.[365]

Besides international conflicts, the usage of Ukrainian cyberspace has also been marked by illegal trade markets, and there are conflicting sources regarding Ukraine's importance as an organ and weapon trafficking hub. In the aftermath of the downfall of the Union of Soviet Socialist Republics (USSR) in 1991, Ukraine inherited a vast stock of Soviet armaments with an estimated value of USD 89 billion. These weapons were then sold on the black market and trafficked out of the country,[366] an event that led to the cementing of such markets in Ukrainian grounds and, eventually, in Ukrainian cyberspace.

---

[362]MATAMIS, J. **False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War • Stimson Center**. Available at: https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/. Accessed on: May 27, 2024.

[363]THE INFOGRAPHICS SHOW. **How Russia is Attacking Ukraine With the Dark Web**. Available at: https://www.YouTube.com/watch?v=3Co4LDm4jx4. Accessed on: May 29, 2024.

[364]*Ibidem.*

[365]*Ibidem.*

[366]OVERHAUL. **What Ukraine's weapons black market means for supply chains**. Available at: https://overhaul.com/ukraine-weapons-black-market-supply-chains/. Accessed on: May 27, 2024.

After receiving a large volume of weapon donations due to the threat of war, supposed Ukrainian sellers have been advertising this weaponry on the black market Although the Global Initiative Against Organized Crime has found that many of these listings are fake and multiple are of Russian sellers posting in Ukrainian with the aid of online automatic translation programs.[367]

The Russian Foreign Ministry also claims that Ukraine is the world leader of black transplants[368], with organs being traded online and offline.[369] However, Ukrainian Vox claims that these allegations are false and are an attempt to manipulate the general public's opinion of the country.[370]

Having begun its operations in Ukraine in 2007[371], the United Nations Office on Drugs and Crime has worked to "mitigate the risks associated with drugs, corruption and organized crime to contribute to Ukraine's sustainable development, recovery and rule of law, in line with UNODC's mandate and international standards."[372] Ukraine is also a party to the Budapest convention on cybercrime,[373] a criminal justice treaty that encourages cooperation between nations in the cyber realm

---

[367]GLOBAL INITIATIVE AGAINST ORGANIZED CRIME. **Monitoring illicit arms flows from the conflict in Ukraine.** Available at: https://riskbulletins.globalinitiative.net/ukr-obs-001/01-monitoring-illicit-arms-flows-from-the-conflict-in-ukraine.html. Accessed on: May 27, 2024.

[368]Black transplants are illegal organ transplants.

[369]MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION. **The world leader of black transplants: in Ukraine, organs are traded online and offline**, "Rossiiskaya Gazeta", August 7, 2023. Available at: https://mid.ru/en/foreign_policy/news/1899824/. Accessed on: May 27, 2024.

[370]VOX UKRAINE. **FAKE: Ukraine is the world leader in "black transplantology" article**. Available at: https://voxukraine.org/en/fake-ukraine-is-the-world-leader-in-black-transplantology-article. Accessed on: May 27, 2024.

[371]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC Programme Office in Ukraine**. Available at: https://www.unodc.org/poukr/index.html. Accessed on: May 27, 2024.

[372]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC in Ukraine Factsheet**. Available at: https://www.unodc.org/poukr/uploads/documents/UNODC_in_Ukraine_Factsheet/UNODC_in_Ukraine_Factsheet_EN.pdf. Accessed on: May 27, 2024.

[373]COUNCIL OF EUROPE. **Details of Treaty No.185**. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Accessed on: May 27, 2024.

and provides procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards.[374]

[374]ICLTC AUSTRALIA. **A new look at the Budapest Convention on Cybercrime**. Available at: https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en#:~:text=185. Accessed on: May 27, 2024.

6 OBSERVER ORGANIZATIONS

Although lacking any voting power, prominent and important agents, with relevance in the cybersphere, supply Member States with the necessary expertise, experience and information to further understand the topic and its intricacies. It is through the observer organizations that the true understanding of cyberspace comes, and thus, they sustain great relevance in upkeep the safety of the interconnected world.[375]

6.1 CENTRE FOR THE STUDY OF EXISTENTIAL RISK – CSER

Image 10: The Centre for the Study of Existential Risk.

Source: The Centre for the Study of Existential Risk.[376]

A Cambridge University interdisciplinary research center dedicated to the study and mitigation of existential risks, the Centre for the Study of Existential Risk (CSER) aims to reduce the risk of human extinction or civilizational collapse, working to understand the risks associated with new technologies and its relationship with human

[375]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Inter-governmental bodies.** Available at: https://www.unodc.org/unodc/es/international-cooperation/inter-governmental-bodies.html. Accessed on: May 31, 2024.
[376]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **About us**. Available at: https://www.cser.ac.uk/about-us/. Accessed on: May 8, 2024.

activity, developing methodological toolkits to identify and evaluate future extreme risks. A part of the Institute for Technology and Humanity (ITH), being launched in 2023 to support world-leading research and teaching that seeks to investigate and shape technological transformations and the opportunities and challenges they pose for our world.[377]

The global community fostered by the CSER involves academics, technologists and policymakers that exam and use their integrated insights on aspects of existential risk, with collaborators such as the Cambridge Conservation Initiative, the Leverhulme Centre for the Future of Intelligence (CFI), the Global Challenges Foundation, the GCR Institute, the Munich Centre for Mathematical Philosophy (MCMP), the Future of Life Institute, the Future of Humanity Institute, the Centre for Research in the Arts, Sciences and Humanities (CRASSH), the Centre for Human-Compatible AI, and the Graduate School of Advanced Integrated Studies in Human Survivability (GSAIS).[378]

The center works across six main areas of research, those being: A Science of Global Risk; Biology, Biotechnology and Global Catastrophic Risks; Extreme Risks and the Global Environment; Risks from Artificial Intelligence; Global Justice and Global Catastrophic Risk; Managing Extreme Technology Risks.[379]

The “A Science of Global Risk” research project works on the development and implementation of a model systematic approach to identify, manage and mitigate risks that present themselves in a global class. Working towards producing concrete proposals for risk management that could be implemented within the existing policy

---

[377] *Ibidem.*

[378] CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **About us**. Available at: https://www.cser.ac.uk/about-us/. Accessed on: May 8, 2024.

[379] CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Our research**. Available at: https://www.cser.ac.uk/research/. Accessed on: May 8, 2024.

landscape, the project divides itself in three intersections, the Forecasting and Modelling Global Risk, the Designing Practical Solutions for the Management of Global Risk and Growing the User Community or the Science of Global Risk.[380]

These methods for studying global risks and their respective worst-case scenarios can be observed on “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation” report, in which risks are analyzed so that harmful uses and delays in the realization of the beneficial applications of Artificial Intelligence (AI) can be prevented.[381]

“Biology, Biotechnology and Global Catastrophic Risks” observes the development of the engineering biology field whilst researching the framework that governs genetically modified organisms, including both formal regulatory and normative frameworks. Combining the studies of cybersecurity and biosecurity with the purpose of identifying areas in which the “Cyber Biosecurity” intersection could result in risk-multipliers, this part of the project hopes to establish common methodologies for the two fields to work together more effectively, avoiding catastrophic risks in the future.[382]

Furthermore, considering that military actors are still one of the biggest funders of biological research and that some of the most significant risks humanity has faced have come from weaponized biology, involving the military application of emerging biotechnologies

---

[380]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **A Science of Global Risk.** Available at: https://www.cser.ac.uk/research/science-global-risk/. Accessed on: May 8, 2024.
[381]BRUNDAGE, Miles, et al.**The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation. Future of Humanity Institute, et al. February, 2018.** Available at: https://arxiv.org/pdf/1802.07228.pdf. Accessed on: March 20, 2024.
[382]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Biology, Biotechnology and Global Catastrophic Risks.** Available at: https://www.cser.ac.uk/research/global-catastrophic-biological-risks/. Accessed on: May 8, 2024.

intend on better comprehending where military investments and research are headed within the biotechnology field, so that interventions regarding the future international environment could be done more effectively.[383]

The “Extreme Risks and the Global Environment” project monitors the impact of human activity and technology on the planet, which focuses on climate change and ecosystem collapse, pointing out the effects of such nature-related issues on international society. The research team works towards the development of strategies to address environmental risks with a global community of academics, technologists, and policymakers.[384]

In “Risks from Artificial Intelligence”, the Centre works within a community interested in safe and globally beneficial AI. The research explores the favorable applications of AI across the world, the use of artificial intelligence on emerging threats and its part in global cybersecurity. Considering the continuous evolution in the AI field, the researchers foresee that safety and security-related issues might appear if AI systems take over some domains of human life.[385]

Moreover, even though the presence of artificial intelligence systems causes some uncertainty within the global community, the project observes that it is more useful towards safe and beneficial intelligence systems, with serious effort being dedicated to lay the groundwork for the safety of future systems.[386]

---

[383]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Biology, Biotechnology and Global Catastrophic Risks.** Available at: https://www.cser.ac.uk/research/global-catastrophic-biological-risks/. Accessed on: May 8, 2024.
[384]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Extreme Risks and the Global Environment.** Available at: https://www.cser.ac.uk/research/extreme-risks-and-global-environment/. Accessed on: May 8, 2024.
[385]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Risks from Artificial Intelligence.** Available at: https://www.cser.ac.uk/research/risks-from-artificial-intelligence/. Accessed on: May 8, 2024.
[386]*Ibidem.*

“Global Justice and Global Catastrophic Risk” works with the presence of inequality, corruption and structural discrimination as drivers of global risk, researching to better understand how issues related to distributive, procedural and relational Justice act as drivers of global risk. The difficulties created by injustice on a global level prevent appropriate risk management actions and how risks are perceived, disempowers those affected by such injustices, slows the process of recovery from disasters, and others.[387]

Finally, the “Managing Extreme Technological Risks” research area focuses on identifying, managing and mitigating risks associated with emerging technologies whose impact threatens human extinction or civilization collapse. Considering the ever-present possibility of the end of civilization within a few generations, researchers take in regard the interests of future generations as a motivation for this study.[388]

Whilst working alongside the United Nations Office on Drugs and Crime (UNODC) on the cybersecurity question, the CSER would demonstrate a key role of bringing the research background to the issues involved, mediating the topics of discussion with the theoretical developments and its real-life applications.[389]

6.2 GOOGLE LLC

Google LLC is an American communications corporation and technology company that operates under the umbrella of Alphabet Inc., a

[387]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Global Justice and Global Catastrophic Risk.** Available at: https://www.cser.ac.uk/research/global-justice-gcr/. Accessed on: May 8, 2024.
[388]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Managing Extreme Technology Risks.** Available at: https://www.cser.ac.uk/research/managing-extreme-technological-risks/. Accessed on: May 8, 2024.
[389]CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **About us**. Available at: ttps://www.cser.ac.uk/about-us/. Accessed on: May 8, 2024.

multinational conglomerate. This holding company ranks among the world's most valuable, boasting a market capitalization of over $ 2 trillion. Notably, it is the only representative from the Communications Services sector to rank in the top five.[390]

Offering a vast range of products and services, Google's tools are essential for the daily interactions of many internet users, serving as a web browser, search engine, email service, video sharing platform, and beyond, while also collecting private data and information. For example, Google Drive enables users to store personal documents, sensitive images, and even share pirated files related to movies or music.

Hence, Google reveals itself to be an extension of cyberspace that requires security measures and privacy standards capable of safeguarding users' interactions – from personal access to sophisticated state systems – against malicious attacks. In response, the platform developed the Google Security Research Project, an open-source database designed to identify security vulnerabilities, aiming to fix bugs and anticipate cyber threats.[391] Through this initiative, the company has made significant efforts to promote innovations in cybersecurity.

Google asserts that its products and services can only be valuable if they are secure. To achieve this, it adopts an approach that seeks to protect people, companies, and governments; empower society to face cybersecurity risks; and develop advanced technologies, such as

[390] FINANCECHARTS. **Biggest Companies in the World by Market Cap for May 2024**. FinanceCharts.com, 2024. Available at: https://www.financecharts.com/screener/biggest. Accessed on: May 26, 2024.
[391] RAWAL, Bharat; EBERHARDT, Gabrielle; LEE, Jaein. **Cybersecurity Snapshot: Google, Twitter, and Other Online Databases**. Journal of Advanced Computer Science & Technology, vol. 5, no. 1, pp. 14-22, Amman, Jordan, 2016. Available at: https://www.sciencepubco.com/index.php/JACST/article/view/6181. Accessed on: May 28, 2024.

machine learning, hardware, cloud computing or even international quantum computing standards.[392]

Given this, the company is at the forefront of employing new technologies to mitigate cyber threats, whether through secure web browser navigation mechanisms, reCAPTCHA bot and fraud management solutions, or specialized task forces like Project Zero, Google Bug Hunter, and Google Play Protect.[393]

Advanced Artificial Intelligence (AI) systems can be highly effective tools for detecting and mitigating software vulnerabilities. In this sense, the Google Bard project utilizes Large Language Models (LLM) to demonstrate their versatility to comprehend code semantics and identify potential security risks.[394] Moreover, the Google Cloud Console (GCC) is employed for digital protection purposes, acting as a supervised machine learning platform that analyzes datasets, identifies patterns, makes decisions, and offers predictions.[395]

In turn, Google's software-based authenticator provides a two-factor token mechanism that increases the complexity for the attacker. The Google Authenticator is particularly popular and easy to use, not requiring an Internet connection while supporting Time-based OneTime Password (TOTP) and HMAC-based One-Time Password (HOTP).[396]

---

[392]GOOGLE. **Google Cybersecurity Innovations**. GOOGLE, 2023. Available at: https://safety.google/cybersecurity-advancements/. Accessed on: May 28, 2024.
[393]*Ibidem*.
[394]GUPTA, Maanak *et al*. **From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy**. IEEE Access, vol. 11, 2023. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10198233. Accessed on: May 28, 2024.
[395]OPARA, Emmanuel. **Cloud-based machine learning and sentiment analysis**. Georgia Southern University, Statesboro, USA, 2022. Available at: https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=3724&context=etd. Accessed on: May 28, 2024.
[396]PAPASPIROU, Vasilis *et al*. **Cybersecurity Revisited: Honeytokens meet Google Authenticator**. 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 2022. Available at: https://ieeexplore.ieee.org/document/9932907. Accessed on: March 28, 2024.

Finally, the company also aims to foster a digital awareness mindset. Google promotes training courses in cybersecurity and distributes professional certificates to qualified individuals.[397/398] These initiatives are designed to ensure the ongoing restructuring and modernization of its digital protection standards while also enhancing its credibility within the security industry.

Therefore, the importance of Google in this area is evident, as an agent focused on advances in cyber risks and vulnerabilities that could undermine its operations, as well as the users' trust. After all, it is advantageous for Alphabet Inc. to participate in international cybersecurity policy efforts, alongside States and other Big Tech companies.

6.3 INTERNATIONAL CRIMINAL POLICE ORGANIZATION – INTERPOL

The International Criminal Police Organization's (INTERPOL) long cooperation history with the United Nations (UN) was formalized in 1997 and further strengthened in 2004 when the Office of the Special Representative was established, a crucial measure for what would be a qualitative and quantitative joint workforce.[399]

Being the only organization with Mandate and technical infrastructure to work on such demand, it plays a role in the attempt to centralize criminal records helping in detection as cybercrime shows no

[397]GOOGLE. **Google Cybersecurity Certificate**. GOOGLE, 2023. Available at: https://grow.google/certificates/cybersecurity/. Accessed on: May 28, 2024.
[398]GOOGLE. **Growth Academy: AI for Cybersecurity**. GOOGLE, 2023. Available at: https://startup.google.com/programs/growth-academy/cyber-security/. Accessed on: May 28, 2024.
[399]INTERPOL. **Our Partners.** Available at: https://www.interpol.int/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations. Accessed on: March 20, 2024.

borders and online offenses have also taken economic and social impacts on a global scale. To help with local range capacity, the United Nations interposes with hosting countries beforehand.[400]

For 100 years now, what used to be the International Criminal Police Commission has worked as a remote and in-person liaison, a jurisdictional, linguistic and cultural link between police forces worldwide through a secure communications system called I-24/7, which allows real-time, frontline database access.[401]

After computerizing all background information in the late 1980s and working with an automatic fingerprint identification system (AFIS), a DNA profile and facial recognition database was established in the 2000s.[402] INTERPOL aims to include all these tools in a new way to decode the means, meanings and languages of Cybercrime through the Commission for the Control of INTERPOL's Files (CCF) a separate body within the bureau's scope which is responsible for ensuring all processed data to follow strict protection rules.[403/404]

Having security as a primary goal, other than running campaigns to help national police organizations to overcome the challenges of under reported cyber crimes,[405] and serving as primary aid for the Foreign

---

[400]*Ibidem.*

[401]INTERPOL. **Our History.** Available at: https://www.interpol.int/Who-we-are/Our-history#:~:text=We%20began%20as%20the%20International,Police%20Organization%2DINTERPOL%20in%201956. Accessed on: March 20, 2024.

[402]INTERPOL. **Fingerprints.** Available at: https://www.interpol.int/en/How-we-work/Forensics/Fingerprints. Accessed on: March 20, 2024.

[403]INTERPOL. **INTERPOL's contribution to the elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf. Accessed on: March 20, 2024.

[404]INTERPOL. **INTERPOL's Rules on the Processing of Data.** Available at: https://www.interpol.int/content/download/5694/file/24%20E%20RPD%20UPDATE%207%2011%2019_ok.pdf. Accessed on: March 20, 2024.

[405]UNITED NATIONS OFFICE ON DRUGS AND CRIME. **INTERPOL's General Statement.** Available at: https://www.unodc.org/documents/Cybercrime/Presentations/STATEMENTS/GENERAL/INTERPOL.pdf. Accessed on: March 20, 2024.

Terrorist Fighters (FTF) group. They benefited from the promptness of the social media analysis as one of the first main missions on understanding the capabilities of web expanding actions against the human rights[406] the permanent Observer extended at the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, hosted by UNODC.[407]

Together, both parties are aligned to help activate the Strategic Framework (2022-2025) which helps member countries with training, effective combat recommendations on the conversion of types of crime from a palpable to an abstract position.[408]

Looking to maximize success, it is encouraged for member states to act under special projects for analyzing imminent threats and carrying actions of the enhancement of law enforcement, use of existing mechanisms and techniques and narrowing gaps amongst State parties primarily by valuable national police monitoring and communication nets in order to create faster reporting on criminal acts.[409]

These acts are made aware of by the diffusion method, where only involved countries are approached within the network from a critical

---

[406]INTERPOL. **INTERPOL and UN join forces to counter exploitation of the Internet for terrorist activities.** Available at: https://www.interpol.int/News-and-Events/News/2019/INTERPOL-and-UN-join-forces-to-counter-exploitation-of-Internet-for-terrorist-activities. Accessed on: March 20, 2024.

[407]INTERPOL. **INTERPOL's Proposal for the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/INTERPOL_Contribution_to_the_AHC_Concluding_Session.pdf. Accessed on: March 20, 2024.

[408]*Ibidem.*

[409]INTERPOL. **INTERPOL's Contribution to the Comprehensive International Convention on Countering the Use of Information Communications Technologies for Criminal Purposes.** Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf. Accessed on: March 20, 2024.

point also facilitated by the presence of online enterprises, holders of multiple encrypted sources.[410]

Said appreciation for public-private cooperation was brought to a real-life scenario by the recent Operation Synergia. 1,300 growing phishing, malware and ransomware cases were targeted, 31 arrests made, and 70 additional suspects identified with the help of over 50 member countries and five personal sector groups such as Kaspersky Lab.[411/412]

Image 11: Operation Synergia's operational components by percentage.

Source: Interpol.[413]

[410]*Ibidem.*

[411]INTERPOL. **INTERPOL-led operation targets growing cyber threats,** Available at: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats. Accessed on: March 20, 2024.

[412]THE RECORD. **Interpol arrests more than 30 cybercriminals in global 'Synergia' operation.** Available at: ; https://therecord.media/interpol-arrests-cybercriminals-in-large-operation. Accessed on: March 20, 2024.

[413]*Ibidem.*

All participating private venues have been working on dissecting the consequences of Artificial Intelligence to human existence and similar to them INTERPOL has its own Innovation Center which accounts for general AI knowledge, exchange and responsible use counting with adjacent research facilities. to identify requests for an AI R&D programme, in-house common aspects curating processes or outsourcing, harmonizing received content with operational support for a safer tomorrow.[414/415]

6.4 KASPERSKY LAB

Kaspersky - or Kaspersky Lab - is a Russian multinational cybersecurity and antivirus provider, situated in Moscow, Russia, and operated by a holding company[416] in the United Kingdom.[417] It was founded in 1997 by Eugene Kaspersky, Natalya Kaspersky and Alexey De-Monderik and represents one of Russia's biggest service providers in terms of reach.[418]

In regards to some of the organization's history, it began to branch out and reach international markets from 2005 to 2010, right when the dire necessity for services and products concerning cybersecurity

[414]INTERPOL. **INTERPOL Innovation Centre**. Available at: https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre. Accessed on: March 20, 2024.
[415]INTERPOL. **Towards Responsible AI Innovation.** Available at: https://www.interpol.int/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf. Accessed on: March 20, 2024.
[416]A holding company is a company whose primary business is holding a controlling interest in the securities of other companies.
[417] KASPERSKY LAB. **Kaspersky**. Moscow: 2024. Available at: https://www.kaspersky.ru/. Accessed on: May 20, 2024
[418]KASPERSKY LAB. **About**. Moscow: 2024. Available at: https://www.kaspersky.ru/about/. Accessed on: May 20, 2024.

became clear.[419] The first version of the antivirus responsible for establishing the business's status was developed by Eugene Kaspersky in 1989, in response to the Cascade Virus[420].[421/422] After some time, the enterprise would expand and improve on the anti-virus so that it could be shared and presented to a larger, international group of buyers.[423]

When it comes to the products and services provided, they may include, but are not limited to antivirus, malware protection, monitoring of the PC for suspicious program behavior, data security services and many more. As such, by the very nature of their work, the company claims to be aware and engaged in going against any and all malicious agents who might try to breach their clients privacy, and that includes governmental entities: "We are a private company and are not driven by short-term commercial considerations and our activities are not influenced by government entities."[424]

Although the business maintains its position in denying any involvement with spying, data mining, associating with nefarious benefactors behind the scenes and other similar malicious activities, there have been accusations made against them on this matter.[425] In

---

[419]SHACHTMAN, Noah. **Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals**. San Francisco: WIRED. San Francisco, April 19, 2011. Available at: https://www.wired.com/2012/07/ff_kaspersky/. Accessed on: May 19, 2024.

[420]The Cascade virus is a prominent computer virus that was resident written in assembly language, that was widespread in the 1980s and early 1990s. It infected .COM files and had the effect of making text on the screen fall (or cascade) down and form a heap at the bottom of the screen.

[421]FORBES. **#1741 Eugene Kaspersky.** New Jersey: Forbes, April 4, 2024. Available at: https://www.forbes.com/profile/eugene-kaspersky/. Accessed on: May 15, 2024.

[422]KRAMER, Andrew E.; PERLROTH, Nicole. **Expert Issues a Cyberwar Warning**. New York: The New York Times, June 3, 2012. Available at: https://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html?pagewanted=all. Accessed on: May 17, 2024.

[423]Op. Cit., SHACHTMAN, Noah.

[424]KASPERSKY LAB. **Transparency**. Moscow: 2024. Available at: https://www.kaspersky.ru/about/transparency. Accessed on: May 20, 2024.

[425]PERLROTH, Nicole; SANGER, David E. **U.S. Embedded Spyware Overseas, Report Claims**. New York: The New York Times, February 3, 2015. Available at: https://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html. Accessed on: May 15, 2024.

2015, multiple American news outlets alleged Kaspersky had been involved in leaking sensitive information from American users and having ties with the Russian Federal Security Service (FSB).

Not only that, but *The Wall Street Journal*, in 2015, reported that there could be hackers working for the Russian government who used Kaspersky antivirus software to steal classified material from a home computer belonging to a National Security Agency (NSA) contractor.[426/427]

This controversy eventually resulted in the American administrative bodies taking preemptive action against the company, in fear of the possibility that these accusations could be truthful. Therefore, in 2017, the United States' General Services Administration (GSA) removed Kaspersky Lab from its list of vendors authorized to do business with the U.S. government amid further reports by *Bloomberg*[428] and McClatchy DC alleging that Kaspersky Lab had worked on secret projects with the Russian Federation's Federal Security Service (FSB).[429]

Their preemptive measures did not end there, however. On September, 2017, the Department of Homeland Security (DHS) issued an order stating that in 90 days Kaspersky products will be banned from use within the U.S. civilian federal government,[430] citing:

---

[426]LUBOLD, Gordon; HARRIS, Shane. **Russian Hackers Stole NSA Data on U.S. Cyber Defense**. New York: Wall Street Journal, October 5, 2017. Available at: https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108. Accessed on: May 16, 2024.

[427]MATLACK, Carol. **The Company Securing Your Internet Has Close Ties to Russian Spies**. Germany: Bloomberg, March 20, 2015. Germany. Available at: https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies. Accessed on: May 20, 2024.

[428]*Ibidem*.

[429]SHAHEEN, Jeanne (2017-09-04). **The Russian Company That Is a Danger to Our Security**. New York: The New York Times, September 4, 2017. ISSN 0362-4331.

[430]NAKASHIMA, Ellen; GILLUM, Jack. **U.S. bans use of Kaspersky software in federal agencies amid concerns of Russian espionage**. Washington, DC: The Washington Post, September 13, 2017. Available at: https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html. Accessed on: May 16, 2024.

> [concerns] about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks.[431]

It also didn't help that the relations between the United States of America (USA) and the former soviet state were already tense because of the suspicion that the Russian government had somehow interfered with the American elections of 2016. Their accusations were not only limited to the USA, as there have also been alleged reports from the United Kingdom[432], Lithuania[433], The Netherlands[434], Germany[435] and more.

Kaspersky's response during this period of turmoil in their relationship with the international market, came in the form of constant denials of involvement with the Russian government[436] and affirmative

---

[431] *Ibidem*.

[432] JONES, Sam; ARNOLD, Martin. **UK spymasters raise suspicions over Kaspersky software's Russia links**. London: The Financial Times, November 12, 2017. Available at: https://www.ft.com/content/37b7b91c-c79e-11e7-ab18-7a9fb7d6163e. Accessed on: May 19, 2024.

[433] REUTERS. **Lithuania bans Kaspersky Lab software on sensitive computers**. London: December 21, 2017. Available at: https://www.reuters.com/article/us-lithuania-russia-idUSKBN1EF23M/. Accessed on: May 18, 2024.

[434] REUTERS. **Dutch government to phase out use of Kaspersky anti-virus software**. London: May 14, 2018. Available at: https://www.reuters.com/article/us-cyber-netherlands-kaspersky-idUSKCN1IF2NV/. Accessed on: May 19, 2024.

[435] PETKAUSKAS, Vilius. **Fears of Russian spying prompts Germany to ditch Kaspersky**. CyberNews, March 21, 2022. Available at: https://cybernews.com/cyber-war/fears-of-russian-spying-prompts-germany-to-ditch-kaspersky/. Accessed on: May 19, 2024.

[436] GOODIN, Dan. **Kaspersky: Yes, we obtained NSA secrets. No, we didn't help steal them**. Ars Technica. Available at: https://arstechnica.com/information-technology/2017/11/kaspersky-yes-we-obtained-nsa-secrets-no-we-didnt-help-steal-them/. Accessed on: May 19, 2024.

action to ensure their international partners of full clearness and accountability. These affirmative actions came in the form of the transparency initiative[437] and data-center mover to outside of Russia[438].

Firstly, the transparency initiative is a model of activity designed so that it would be easier to make the company accountable for security issues surrounding its products, in which select countries would be able analyze their methods and databases - by allowing third-party analysts to validate its products and other business practices - in order to verify their integrity.[439] These analysts could even be private or public, government administered or private initiative, in nature:

> Transparency Centers serve as facilities for trusted partners to access reviews of the company's code, software updates and threat detection rules, along with other activities. Through them, we provide governments and partners with information on our products and their security, including essential and important technical documentation, for external evaluation in a secure environment. They also serve as a briefing center where trusted stakeholders can learn more about the company's portfolio, engineering and data processing practices. Kaspersky Transparency Centers are operating in Kigali, Kuala

[437]KASPERSKY LAB. **Transparency**. Moscow: 2024. Available at: https://www.kaspersky.ru/about/transparency. Accessed on: May 20, 2024.
[438]KASPERSKY LAB**. Kaspersky completes its data-processing relocation to Switzerland and opens new Transparency Center in North America.** Moscow: November 17, 2020. Available at: https://www.kaspersky.com/about/press-releases/2020_kaspersky-completes-its-data-processing-relocation-to-switzerland-and-opens-new-transparency-center-in-north-america. Accessed on: May 20, 2024.
[439]KASPERSKY LAB. **Transparency**. Moscow: 2024. Available at: https://www.kaspersky.ru/about/transparency. Accessed on: May 20, 2024.

> Lumpur, Madrid, Riyadh, Rome, São Paulo, Singapore, Tokyo, Utrecht, Woburn, and Zurich. At Kaspersky's Transparency Centers, the company provides the opportunity to compile its software from the source code and compare it with the publicly available one.[440]

In conclusion, Kaspersky Lab has made multiple efforts in the fight against malware and in favor of cybersecurity. These actions occurred as active investigations and assistance to international entities, like Interpol[441], or Kaspersky Lab's Global Research and Analysis Team (GReAT), established in 2008, and tasked with investigating cybersecurity threats and other work by malware operations. For that reason, the company is committed to ensure a bright future for further development of digital technology, without the fear of malware operators and malicious practices.

6.5 MASSACHUSETTS INSTITUTE OF TECHNOLOGY – MIT

The Massachusetts Institute of Technology (MIT) is a private land-grant research university located in Cambridge, Massachusetts, established in 1861 in order to accelerate the industrial revolution in the United States of America.[442] As of October 2023, 101 Nobel Laureates have been affiliated with the institution either as alumni, faculty members, or researchers, and it is ranked second place in US News's Best Global

[440] *Ibidem*.
[441] *Ibidem*.
[442] MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About MIT | MIT - Massachusetts Institute of Technology**. Available at: https://www.mit.edu/about/. Accessed on: May 31, 2024.

Universities ranking[443]. MIT comprises five schools: Architecture and Planning; Engineering; Humanities, Arts, and Social Sciences; Management; and Science.[444]

> The MIT community is driven by a shared purpose: to make a better world through education, research, and innovation. We are fun and quirky, elite but not elitist, inventive and artistic, obsessed with numbers, and welcoming to talented people regardless of where they come from.[445]

The computer science program in MIT is currently considered the best in the world,[446] with research being carried throughout multiple subareas, such as Artificial Intelligence (AI) and Machine Learning (ML), communications systems, computer architecture, quantum computing, graphic and visual computing, systems and networking, and others[447]. MIT also offers specialization in the cybersecurity area, exploring information security, ethical and legal practices, and cyber vulnerabilities defenses, while focusing on ensuring the privacy, reliability, and integrity of information systems.[448]

The institution has a history of collaborating with both local and global governments in research projects, as well as with companies,

---

[443]**MASSACHUSETTS Institue of Technology #2 Best Global Universities**. Available at: https://www.usnews.com/education/best-global-universities/massachusetts-institute-of-technology-mit-166683. Accessed on: May 31, 2024.
[444]*Ibidem.*
[445]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About MIT | MIT - Massachusetts Institute of Technology**. Available at: https://www.mit.edu/about/. Accessed on: May 31, 2024.
[446]**QS WORLD University Rankings for Computer Science and Information Systems 2023**. Available at: https://www.topuniversities.com/university-subject-rankings/computer-science-information-systems. Accessed on: May 31, 2024.
[447]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **COMPUTER Science – MIT EECS**. Available at: https://www.eecs.mit.edu/research/computer-science/. Accessed on: June 1, 2024.
[448]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Applied Cybersecurity | Professional Education**. Available at: https://professional.mit.edu/cybersecurrity-old. Accessed on: June 1, 2024.

other universities, non-profits, and a broad range of other institutions. Most international collaborations involve individual members of the faculty and research staff, usually working with students, but MIT may also seek to establish larger working relationships.[449] One such relationship led to the creation of the MIT Lincoln Lab, a federally funded research and development center (FFRDC) in partnership with the government of the United States (U.S.), sponsored by the Department of Defense (DoD).[450]

The Lincoln Lab works in cross-disciplinary teams researches and develops a broad array of advanced technologies to meet critical national security needs, such as ground and space terminals that enable fast data downloads from National Aeronautics and Space Administration (NASA) satellites, high-resolution long-range imaging sensors, beam-combining lasers, and biomedical devices.[451] The Lincoln Lab Cyber Security and Information Sciences groups develop technology that solves demanding U.S. national security problems.[452]

In order to enhance its contribution to the U.S. Government in science, engineering, and education, MIT also boasts an MIT Washington Office, where government officials may consult with the Institute's faculty and administrators on issues that may require technical, scientific, and policy advice.[453]

---

[449]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **MIT Partners**. Available at: https://global.mit.edu/for-partners/. Accessed on: June 1, 2024.
[450]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About | MIT Lincoln Laboratory**. Available at: https://www.ll.mit.edu/about. Accessed on: May 31, 2024.
[451]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About | MIT Lincoln Laboratory**. Available at: https://www.ll.mit.edu/about. Accessed on: May 31, 2024.
[452]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Cyber Security and Information Sciences | MIT Lincoln Laboratory**. Available at: https://www.ll.mit.edu/r-d/cyber-security-and-information-sciences. Accessed on: May 31, 2024.
[453]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **12.1 Relations with Government and Community | Policies**. Available at: https://policies.mit.edu/policies-procedures/120-relations-public-use-mit-name-and-facilities-use/121-relations-government. Accessed on: June 1, 2024.

MIT is committed to producing, disseminating, and preserving knowledge, as well as to working with others to bring this knowledge to bear on the world's great challenges. As a modern university and social institution, the Institute recognizes “an inherent obligation to serve its students, its alumni and alumnae, the professions, the world of scholarship, and society.”[454] As part of this obligation, MIT seeks to serve the community and the nation directly through its faculty and through the use of its facilities and administrative resources whenever there is a compelling need to which it can respond without impairing its primary function.[455]

6.6 META INC.

Meta - as in Meta Platforms, inc. - is an American multinational technology conglomerate and social media platform, specialized in the development of products and services regarding information technology and data retention.[456] Not only that, but it also represents one of the most successful digital media enterprises of the 21 century.

When it comes to Meta’s history, the mother-business first started on February 4, 2004, under the name of “The Facebook” - which was later shortened to Facebook in August 2005 - as a joint effort from Mark Zuckerberg, Eduardo Saverin. The platform's rebranding can be traced back to an initial public offering (IPO)[457], made on January first, 2012,

---

[454]MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **1.1 Mission and Objectives | Policies**. Available at: https://policies.mit.edu/policies-procedures/10-institute/11-mission-and-objectives. Accessed on: June 1, 2024.
[455]*Ibidem.*
[456]**META PLATFORMS, INC.** California: January 4, 2004. Available at: https://about.meta.com/. Accessed on: May 20, 2024.
[457]Which is when shares of a company are sold to private and institutional investors in an attempt to generate funds for a project or expansion.

filled by Facebook[458], with investors composed mainly of investment banks and private interested parties. Anyhow, the accumulated funds generated by this endeavor were more than enough for Mark Zuckerberg[459], CEO and founder of its parent company Facebook, inc., to shift the establishment into broader tech development-oriented activities.

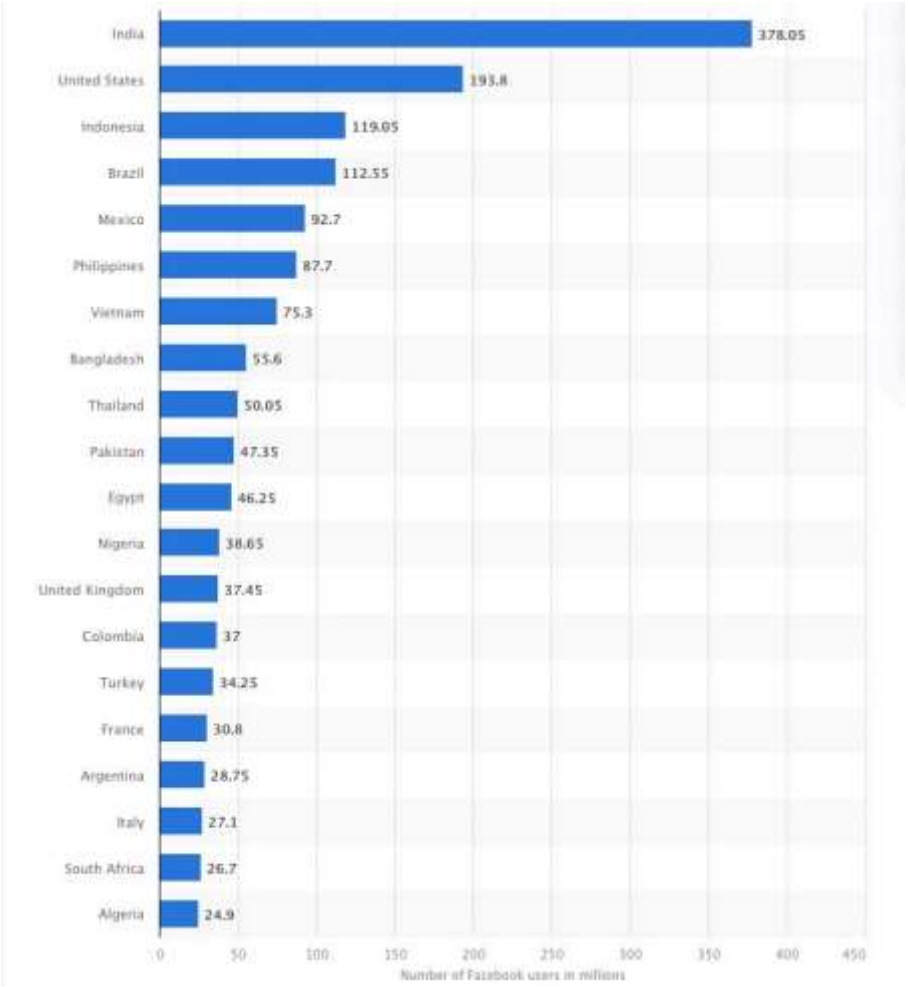
Later, with its official new name, Meta Platforms, inc. would go on to become one of the most successful social media platforms in history, hosting around 2.9 billion monthly active users and making huge amounts of revenue through advertising.[460]

Image 11: Leading countries based on Facebook audience size as of April 2024 (in millions).

[458]UNITED STATES OF AMERICA**. Securities and exchange commission, under the securities act of 1993**. Registration statement. Available at: https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm. Accessed on: May 20,2024.

[459]KIRKPATRICK, David. **The Facebook Effect: The Inside Story of the Company That Is Connecting the World.** New York: Simon & Schuster. Published on June 8, 2010. pp. 20–21. ISBN 978-1-4391-0211-4. Archived from the original on November 12, 2012.

[460]STATISTA RESEARCH DEPARTMENT. **Share of GDP expenditure on research and development in Russia from 2001 to 2020**. Statista, February 17, 2023. Available at: https://www.statista.com/statistics/461754/share-of-gdp-expenditure-on-research-and-development-russia/. Accessed on: May 21, 2024.



Source: Statista.[461]

Although historically Facebook's revenue is mostly from to advertisements, the company, as recently as 2021, with its rebranding, has been working on the development of a cybernetic virtual space for further amplification of human contact and communication through the internet, the Metaverse, which is a billion dollar project with estimates a revenue of $490 billion in 2030.[462/463] This venture into the production of

[461]STATISTA RESEARCH DEPARTMENT. **Share of GDP expenditure on research and development in Russia from 2001 to 2020**. Statista, February 17, 2023. Available at: https://www.statista.com/statistics/461754/share-of-gdp-expenditure-on-research-and-development-russia/. Accessed on: May 21, 2024.

[462]**META PLATFORMS, INC.** California: January 4, 2004. Available at: https://transparency.meta.com/pt-br/metasecurity/threat-disruptions/. Accessed on: May 20, 2024.

[463]STATISTA RESEARCH DEPARTMENT. **Share of GDP expenditure on research and development in Russia from 2001 to 2020**. Statista, February 17, 2023. Available at:

new technologies also comes with a renewed vigor for data security, as more contact with users personal information during the use of the platform constitutes even more risk for data leaks.

When it comes to Meta's background in cybernetic data leaks, despite what the company portrays, Meta has a concerning history of personal users data related issues and transparency.[464] In an effort to further study the effects data leaks have on the financial stability of economic actors in a global scale, students from the Security and Defence quarterly[465] made a case study compiling the many scandals surrounding Meta and its data breaches:

> In 2014, Cambridge Analytica collected Facebook user profiles in unethical and non-legal ways, affecting about 87 million users in the US (Business Insider, 2019). The publicity regarding the incident caused a drop in the company's share price by approximately 7 per cent, on 19 March 2018 (CNBC, 2018).
> On 28 September 2018, Meta revealed a data theft affecting about 2 million Facebook users' date of birth, phone number, search history, and last login location. Even before the official announcement, on 27 September 2018, the share price fell by 3 per cent due to the publicity around the cyberattack (Business Insider, 2018).

https://www.statista.com/statistics/461754/share-of-gdp-expenditure-on-research-and-development-russia/. Accessed on: May 21, 2024.

[464]BEDERNA, Zsolt; SZÁDECZKY, Tamás. **Managing the financial impact of cybersecurity incidents.** Security and Defence Quarterly, v. 41, 2023. Available at: https://securityanddefence.pl/Managing-the-financial-impact-of-cybersecurity-incidents,159625,0,2.html. Accessed on: May 20, 2024.

[465]*Ibidem*.

> On 24 March 2019, a security incident affecting the Instagram service was announced (Facebook, 2019c). On 18 April 2019, new information was revealed. When, on 12 June 2019, CEO Mark Zuckerberg's sent a related email concerning problematic privacy practices, share prices fell 2.9 per cent (Markets Insider, 2019).[466]

With the negative press, in 31 October, 2019, Meta was inspired to create a transparency center[467/468], in order to recover users' belief in the security of their platforms and make it more difficult for malicious groups to usurp their technology in detriment of their clientbase.[469]

Furthermore, there are also issues regarding espionage and alleged misuse of META technologies for the interest of international entities and governments.[470] Meta's internal administrative branch has been made aware of several different attempts regarding the largest known covert influence operations, allegedly related to Russia and China[471], to spy on their databases and, as contingency, resorted to taking down and linking treacherous accounts to their respective responsible bodies of administration:

According to META's report:

---

[466]*Ibidem*.

[467]**META PLATFORMS, INC.** California: January 4, 2004. Available at: https://transparency.meta.com/pt-br/metasecurity/threat-disruptions/. Accessed on: May 20, 2024.

[468]Which consists of an internet page describing their methods for ensuring data security, their many achievements in this line of work, their new technologies designed for protecting users information and their means for dealing with bad actors inside their platform.

[469]*Op. cit.*, Meta platforms, inc.

[470]VOLZ, Dustin; FITZGERALD, Drew; CHAMPELLI, Peter; BROWN, Emma. **U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships.** Published by the Wall Street Journal, May 19, 2024. Available at: https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320?st=wy5kmsu7l8jrvvz&reflink=desktopwebshare_permalink. Accessed on: May 21, 2024.

[471]**META PLATFORMS, INC.** California: January 4, 2004. Available at: https://about.fb.com/news/2023/08/raising-online-defenses/. Accessed on: May 20, 2024.

China: We recently took down thousands of accounts and Pages that were part of the largest known cross-platform covert influence operation in the world. It targeted more than 50 apps, including Facebook, Instagram, X (formerly Twitter), YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, VKontakte, Vimeo, and dozens of smaller platforms and forums. For the first time, we were able to tie this activity together to confirm it was part of one operation known in the security community as Spamouflage and link it to individuals associated with Chinese law enforcement.

Russia: We also blocked thousands of malicious website domains as well as attempts to run fake accounts and Pages on our platforms connected to the Russian operation known as Doppelganger that we first disrupted a year ago. This operation was focused on mimicking websites of mainstream news outlets and government entities to post fake articles aimed at weakening support for Ukraine. It has now expanded beyond initially targeting France, Germany and Ukraine to also include the US and Israel. This is the largest and the most aggressively-persistent Russian-origin operation we've taken down since 2017. In addition to new threat research, we're also publishing our enforcement and policy recommendations for

addressing the abuse of the global domain name registration system.[472]

In conclusion, Meta platforms, inc., in appreciation of their internal motto “Move fast with stable infrastructure”[473], understands the nature of the concerns surrounding data security in their platforms and technologies. For that reason, the company has taken measures to ensure their users personal information remains secure, in a transparent and collaborative manner, and has taken steps into the creation of tools for handling the more nefarious agents inside their platforms.[474]

6.7 TENCENT HOLDINGS LTD.

Shenzhen based Tencent Holding Inc. is a Chinese internet services and retailing company, founded in 1998 by Pony Ma (Ma Huateng; Chinese: 马化腾), owner of China’s social media giant WeChat and the world’s largest video game vendor.[475]/[476] It runs internationally acclaimed and popular games such as PUBG, Call of Duty and League of Legends,[477] and through WeChat, it allows Chinese nationals to

[472]*Ibidem*.
[473]BAER, Drake. **Mark Zuckerberg Explains Why Facebook Doesn't 'Move Fast And Break Things' Anymore**. Business insider. May 2, 2024. Available at: https://www.businessinsider.com/mark-zuckerberg-on-facebooks-new-motto-2014-5. Accessed on: May 20, 2024.
[474]**Meta platforms, inc.** United States of America. Menlo Park, California. Founded January 4, 2004. Available at: https://about.fb.com/news/2023/05/how-meta-protects-businesses-from-malware/. Accessed on: May 20,2024.
[475]TENCENT. **About us.** Shenzhen: 2024. Available at: https://www.tencent.com/en-us/about.html. Accessed on: May 27, 2024.
[476]GILBERT, Ben. **The biggest game company in the world isn't Nintendo — it's a Chinese company that has a piece of everything from 'Fortnite' to 'League of Legends'.** New York: Business Insider, October 2019. Available at: https://www.businessinsider.com/what-is-tencent-games-explainer-2019-8#whats-the-deal-with-tencent-1. Accessed on: May 27, 2024.
[477]TENCENT GAMES. **Introduce**. Shenzhen: 2024. Available at: https://www.tencentgames.com/introduce.html. Accessed on: May 27, 2024.

exchange messages, shop, watch videos, play games, order food and taxis and more within one single app, amassing over 1.3 billion monthly users.[478]

Image 12: WeChat's shopping service (L), its food deliveries, hotel bookings, and cinema bookings (center), and its investment page.

Source: BBC.[479]

Although the large user base of the messaging application proves its popularity, international entities have shown concerns over privacy and data security of its billion domestic and foreign users. To use the app, for instance, one has to give it seventy-two permissions, including camera, audio and location tracking, and going as far as acquiring device identifiers - IMEI, IMSI, model, operating system and contained code.[480]

---

[478]THOMALA, Lai Lin. **Number of monthly active WeChat users from 4th quarter 2013 to 4th quarter 2023.** Statista, April 8, 2024. Available at: https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/#:~:text=The%20number%20of%20Tencent's%20WeChat,1.3%20billion%20monthly%20active%20users. Accessed on: May 29, 2024.

[479]HOSKINS, Peter; WANG, Fan. **WeChat: Why does Elon Musk want X to emulate China's everything-app?.** UK: BBC News, July 29, 2023. Available at: https://www.bbc.com/news/business-66333633. Accessed on: May 29, 2024.

[480]RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. WeChat privacy concerns and data collection. *In:* RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. **TikTok and WeChat: Curating and controlling global information flows**. Australia: Australian Strategic Institute, September 1, 2020. p. 43-46. Available at: https://www.jstor.org/stable/resrep26120.8?seq=1. Accessed on: May 27, 2024.

These tracking permissions allowed the Chinese Communist Party to send notification and classify Chinese citizens on their exposure to the virus during the COVID-19 pandemic.[481]

Additionally, as the app uses client to server (C2S) encryption, instead of end-to-end (E2E), to protect the messages sent through the app from third parties, it doesn't protect it from the provider or anyone who is granted access to the physical or digital central server.[482] This raises concerns, especially considering China's Cybersecurity Law determining that upon request any information must be provided to authorities given undefined "national security concerns".[483] It was this kind of concern that lead WeChat to be banned in the USA in 2020, with then president Donald Trump saying:

> (...) WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information. In addition, the application captures the personal and proprietary information of Chinese nationals visiting the United States, thereby allowing the Chinese Communist Party a mechanism for

[481]KO, June. **The Chinese government used technology to get a grip on coronavirus – and take control of its people.** Hong Kong: The Independent, April 14, 2020. Available at: https://www.independent.co.uk/voices/coronavirus-china-technology-mass-surveillance-privacy-human-rights-a9463586.html. Accessed on: May 27, 2024.

[482]RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. WeChat privacy concerns and data collection. *In:* RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. **TikTok and WeChat: Curating and controlling global information flows**. Australia: Australian Strategic Institute, September 1, 2020. p. 43-46. Available at: https://www.jstor.org/stable/resrep26120.8?seq=1. Accessed on: May 27, 2024.

[483]Throughout China's Cybersecurity Law from 2016 there is extensive mentions to national security concerns, a term that is not defined anywhere else in said law and that foreign critics fear might be used by the government to acquire access to companies' intellectual property and users' private data, as article 28, for example, says that "Network operators shall provide technical support and assistance to public security organs' and state security organs' lawful activities preserving national security and investigating crimes".

> keeping tabs on Chinese citizens who may be enjoying the benefits of a free society for the first time in their lives. For example, in March 2019, a researcher reportedly discovered a Chinese database containing billions of WeChat messages sent from users in not only China but also the United States, Taiwan, South Korea, and Australia.[484]

Although appearing to work alongside the People's Republic of China, Tencent also seems to get into conflict with its own governmental body. A former vice minister of public relation was expelled from the CCP after soliciting information on fellow politicians, and a project to predict political succession caught Beijing's attention in a bad light.[485]

The Chinese conglomerate is the second largest investor in R&D in the country, and 19th overall around the globe, placing above more well-known companies like Ford Motors and BMW.[486] Their most recent scientific venture has led to the new palm payment technology, allowing a user to pay and access services "with a simple hand motion". According to the company, the technology, still in its early trail phase, is simple to use and provides many benefits.[487] Thus:

---

[484]TRUMP, Donald J. **Executive Order on Addressing the Threat Posed by WeChat.** Washington DC: The White House, August 6, 2020. Available at: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/. Accessed on: May 27, 2024.
[485]CHEN, Lulu Yilun. **WeChat Is China's Most Beloved (and Feared) Surveillance Tool.** United States: Bloomberg, July 12, 2022. Available at: https://archive.is/hQaSB#selection-3813.0-3821.336. Accessed on: May 27, 2024.
[486]NINDL, Elisabeth. *et al.* **The 2023 EU Industrial R&D Investment Scoreboard.** Luxembourg: Publications Office of the European Union, 2023. Available at: https://dx.doi.org/10.2760/506189. Accessed on: May 27, 2024.
[487]TENCENT. **Weixin's Palm Scan Payments Is Like Waving at a Friend.** Shenzhen: Tencent, 2024. Available at: https://www.tencent.com/en-us/articles/2201785.html. Accessed on: May 27, 2024.

> To activate, users align their palm with the sensor on the palm scan device, then scan the screen's QR code to register on their mobile phones. Upon successful registration, users can make payments by scanning their palms directly. After making a payment, users receive an instant notification of the deducted amount on their mobile phones.[488]

That said, Tencent's importance in both the Chinese market and society is undeniable. However, it struggles to obtain the trust of many foreign governments, fearing a potential leak of their nationals' personal data to the authoritarian power.[489] Through its activity with UNODC, the merchant giant must collaborate to ensure the safety of its products while promoting safer experiences for its billions of service users.

[488] *Ibidem.*

[489] BBC Click. **Should You Be Worried About WeChat?.** 2020. 5min19s**.** Available at: https://www.YouTube.com/watch?v=El8-fYmCpL4. Accessed on: May 29, 2024.

7 CONCLUSIONS

Establishing a line of thought to contemplate a new modern reality, this document provided an attempt to draft a provisioning scenario on how to face a new modality of crime. But also facilitating tools have surged due to the implementation of technology in human daily life. It is crucial to ascertain that all private and public parties have been playing and are currently committed to enhancing quality activity overview the future of digital institutionalization and legal frameworks that actually represent an accordingly perspective to physical statistical inspirational story lines.

As of the necessity for the enactment of an *Ad Hoc* Committee for dealing with all impending threats against a graceful flow of a future envisioned for global States, the participation of all these nations and sympathizing actions from private enterprises for economical, more effective, wide-reaching, and speedier results. All aforementioned characteristics deemed as indispensable for safeguarding a non-dismantling track as definitions are yet to be complete, solidified and adapted to each individual civil lifestyle.

Nonetheless, it is important to note that the scope of the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes travels between abstract and factual aspects to ensure geopolitically significant results. Hence, addressing negative creations which might resurrect from attempts of innovation and reflect on monopolistic tendencies which ought to turn more inclusive perspectives around will show avant-garde odds.

Lastly, considering all characters and the responsibility of the committee members to take stance on presented issues, it is encouraged

that all delegations through thorough research covering the content that has been presented adjacent to the themes and the positions of active and observer members find supportive tools for diplomatic debate and simulation focal agenda topics. Even so as it is also not discouraged the discussion of specific issues contemplating further digested profiles.

REFERENCES

AA ENERGY. **Turkey fights cybercrimes with own capabilities.** Available at: AA Energy. Accessed on: March 26, 2024.

AFRICAN UNION. **African Union Convention on Cyber Security and Personal Data Protection.** Malabo, 2014. Available at: African Union. Accessed on: May 20, 2024.

AGUILAR, Juan Antonio Manuel. **Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad**. URVIO, Revista Latinoamericana de Estudios de Seguridad, no. 25, pp. 24-40, Quito, Ecuador, 2019 December 19, 2015. Available at: Scielo. Accessed on: May 26, 2024.

AI BUSINESS. **Turkey publishes its National Artificial Intelligence Strategy.** Available at: AI Business. Accessed on: May 26, 2024.

AISHAMMARI, Tareq Saeed; SINGH, Harman Preete. **Preparedness of Saudi Arabia to Defend Against Cyber Crimes**: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Boston University Press, Boston, October 30, 2023.

ARTICLE 19. **Islamic Republic of Iran:** Computer Crimes Law. Article 19, London, 2012.

AUSWÄRTIGES AMT. **UNODC - United Nations Office on Drugs and Crime.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

BAER, Drake. **Mark Zuckerberg Explains Why Facebook Doesn't 'Move Fast And Break Things' Anymore. Business insider.** May 2, 2024. Available at: Business Insider. Accessed on: May 20, 2024.

BAEZNER, Marie; ROBIN, Patrice. **Stuxnet**. Center for Security Studies (CSS), ETH Zürich, Zurique, v. 4, October 18, 2017.

BAKERMCKENZIE. **Global Data Privacy and Cybersecurity Handbook.** Available at: BAKERMCKENZIE. Accessed on: May 21, 2024.

BALMFORTH, T. **Exclusive: Russian hackers were inside Ukraine telecoms giant for months.** Reuters, January 5, 2024. Available at: Reuters. Accessed on: May 27, 2024.

BBC Click. **Should You Be Worried About WeChat?.** 2020. 5min19s. Available at: YouTube. Accessed on: May 29, 2024.

BEAUVAIS, Camille. **Dark tourism, "Netflix tourism": stakes and conflicts of actors in Medellin**. (Mega) Evénements urbains et tourisme: pratiques touristiques et organisation spatiale, vol. 22, 2022. Available at: Open Edition Journals. Accessed on: May 26, 2024.

BEDERNA, Zsolt; SZÁDECZKY, Tamás. **Managing the financial impact of cybersecurity incidents. Security and Defence Quarterly, v. 41, 2023**. Available at: Security and Defence. Accessed on: May 20, 2024.

BERG, Ryan; ZIEMER, Henry. **The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment**. Center for Strategic and International Studies, Washington, DC, 2021 November 19. Available at: CSIS. Accessed on: May 26, 2024.

BLUM, Yehuda Z. **Russia Takes Over the Soviet Union's Seat at the United Nations.** Oxford: European Journal of International Law, Oxford University Press, August 2, 1999. Archived from the original on March 12, 2005. Available at: Web Archive. Accessed on: May 20, 2024.

BRANDS, M. **Cybersecurity Laws and Legislation (2023) | ConnectWise**. Available at: Connect Wise. Accessed on: May 31, 2024.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Diário Oficial da União. Brasil, ano 23, n. 245, 1, p. 10. 26 dezembro 2023.** Available at: GOV.BR. Accessed on: May 21, 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018.** Available at: GOV.BR. Accessed on: May 21, 2024.

BRUCE M., LUSTHAUS J., KASHYAP R., PHAIR N, VARESE F. **Mapping the global geography of cybercrime with the World Cybercrime Index**. PLoS ONE 19(4): e0297312. Available at: Doi Foundation. Accessed on: May 27, 2024.

BRUNDAGE, Miles, et al.**The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation.** Future of Humanity Institute, et al. February, 2018. Available at: Arxiv. Accessed on: May 21, 2024.

BULLER, Alicia. **Saudi Arabia Strengthens Its Cybersecurity Posture**. Dark Reading, December 28, 2023. Available at: Dark Reading. Accessed on: May 27, 2024.

CENTER FOR HUMAN RIGHTS IN IRAN. **The National Information Network (National Internet)**. Center For Human Rights in Iran, November 10, 2014. Available at: Iran Human Rights. Accessed on: May 27, 2014.

CENTRAL INTELLIGENCE AGENCY. **The World Factbook:** Iran. Central Intelligence Agency, May 22, 2024. Available at: CIA. Accessed on: May 27, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **A Science of Global Risk.** Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **About us**. Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Biology, Biotechnology and Global Catastrophic Risks.** Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Extreme Risks and the Global Environment.** Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Global Justice and Global Catastrophic Risk.** Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Managing Extreme Technology Risks.** Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Our research**. Available at: CSER. Accessed on: May 8, 2024.

CENTRE FOR THE STUDY OF EXISTENTIAL RISK. **Risks from Artificial Intelligence.** Available at: CSER. Accessed on: May 8, 2024.

CHEN, Chi; ZHOU, Leo. **Global companies must assess their data compliance maturity levels and determine whether processes can be improved.** Shanghai: Ernst & Young, July 18, 2022. Available at: EY. Accessed on: May 27, 2024.

CHEN, Lulu Yilun. **WeChat Is China's Most Beloved (and Feared) Surveillance Tool.** United States: Bloomberg, July 12, 2022. Available at: Bloomberg. Accessed on: May 27, 2024.

CHINA LAW TRANSLATE. **2016 Cybersecurity Law.** November 07, 2016. Available at: China Law Translate. Accessed on: May 27, 2024.

CHINA POWER TEAM. **How Web-connected is China?.** China Power, April 18, 2019. Available at: ChinaPower Project. Accessed on: May 27, 2024.

CLARANET. **Cibersegurança: veja os setores mais críticos no Brasil.** Available at: Claranet. Accessed on: May 21, 2024.

COCKBURN, Patrick. **Boris Kagarlitsky, a member of the Russian Academy of Sciences Institute of Comparative Politics, writing in the weekly Novaya Gazeta, says that the bombings in Moscow and elsewhere were arranged by the GRU**. Independent.co.uk. Archived from the original on 27 August 2009. Available at: Web Archive. Accessed on: May 21, 2024.

COLOMBIA. **Lineamientos de política para Ciberseguridad y Ciberdefensa**. Bogotá: Documento Consejo Nacional de Política Económica y Social – CONPES 3701, 2011. Available at: Government of Colombia. Accessed on: May 26, 2024.

COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **About us: Our mission & vision**. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence. Available at: CCDCOE. Accessed on: May 22, 2024.

COUNCIL OF EUROPE. **Cybercrime policies/strategies**. Available at: Council of Europe. Accessed May 24, 2024.

COUNCIL OF EUROPE. **Details of Treaty No.185**. Available at: Council of Europe. Accessed on: May 27, 2024.

COUNCIL OF EUROPE. **Germany Cybercrime Community**. Available at: Council of Europe. Accessed on: May 23, 2024.

COUNCIL OF EUROPE. **Israel:** Status regarding Budapest Convention. Council of Europe, 2024. Available at: Council of Europe. Accessed on: May 27, 2024.

COUNCIL OF EUROPE. **Saudi Arabia**: Cybercrime policies/strategies. Council of Europe, 2020. Available at: Council of Europe. Accessed on: May 27, 2024.

COUNCIL OF EUROPE. **Serbia**: Cybercrime legislation. Council of Europe, 2020. Available at: Council of Europe. Accessed on: May 27, 2024.

COUNCIL OF EUROPE. **Serbia**: Cybercrime policies/strategies. Council of Europe, 2020. Available at: Council of Europe. Accessed on: May 27, 2024.

COUNCIL OF EUROPE. **The Budapest Convention (ETS No. 185) and its Protocols.** Budapest, 2001. Available at: Council of Europe. Accessed on: May 20, 2024.

CSIS. **Significant Cyber Incidents | Center for Strategic and International Studies**. Available at: CSIS. Accessed on: May 27, 2024.

CYBERSECURITY PHILIPPINES CERT. **A credible and trusted leader in Cybersecurity.** Available at: Philippines CERT. Accessed on: May 18, 2024.

CYBERSECURITY PHILIPPINES CERT. **Digital Forensics and Incident Response.** Available at: Philippines CERT. Accessed on: May 18, 2024.

DAILY SABBAH. **Türkiye becomes world's most cyber targeted region in 2023.** Available at: Daily Sabbah. Accessed on: May 25, 2024.

DARKOWL. **Darknet Cartel Associated Marketplaces**. Denver, USA, 2002. Available at: Darkowl. Accessed on: May 26, 2024.

DAVIDSON, Lincoln E. **‘Internet Plus’ and the Salvation of China’s Rural Economy.** Arlington: The Diplomat, July 17, 2025. Available at: The Diplomat. Accessed on: May 27, 2024.

DEPARTMENT OF HOMELAND SECURITY. **Cybersecurity / Information Analysis R&D | Homeland Security**. Available at: DHS. Accessed on: May 31, 2024.

DEPARTMENT OF HOMELAND SECURITY. **Cybersecurity**. Available at: DHS. Accessed on: May 31, 2024.

DEPARTMENT OF JUSTICE, OFFICE OF CYBERCRIME. **Republic Act No. 10175.** Available at: Department of Justice. Accessed on: May 20, 2024.

DEPARTMENT OF JUSTICE, OFFICE OF CYBERCRIME. **Republic Act No. 10175.** Available at: Department of Justice. Accessed on: May 20, 2024.

DEUTSCHLAND.DE. **Rules for using artificial intelligence and Europe.** Available at: DEUTSCHLAND.DE. Accessed on May 23, 2024.

DFG - DEUTSCHE FORSCHUNGSGEMEINSCHAFT. **DFG, German Research Foundation.** Available at: DFG. Accessed on: May 23, 2024.

DIGITAL TRANSFORMATION OFFICE. **National Artificial Intelligence Strategy 2021-2025.** Available at: Digital Transformation Office. Accessed on: May 26, 2024.

DOYLE, C. **Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.** [s.l: s.n.]. Available at: Congressional Research Reservice. Accessed on: May 31, 2024.

DUPUY, Pablo Casas (org.). **Violence, crime, and illegal Arms trafficking in Colombia**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: United Nations Office on Drugs and Crime. Accessed on: May 26, 2024.

ENACT. **Global Organized Crime Index - Philippines.** Available at: ENACT. Accessed on: May 20, 2024.

EURONEWS. **Rise in cyber attacks on German business costing billions of Euros.** Available at: EURONEWS. Accessed on: May 23, 2024.

EUROPEAN COMMISSION. **Horizon Europe**. Available at: European Commission. Accessed on: May 21, 2024.

EUROPEAN PARLIAMENT. **EU AI Act: first regulation on artificial intelligence | Topics.** Available at: European Parliament. Accessed on: May 23, 2024.

EUROPEAN PARLIAMENT. **Fighting cybercrime:** new EU cybersecurity laws explained. Available at: European Parliament. Accessed on: May 23, 2024.

EUROPEAN PARLIAMENT. **The NIS2 Directive.** Available at: European Parliament. Accessed on May 23, 2024.

EUROPEAN UNION. **Promoting irresponsible AI: lessons from a Brazilian bill.** Available at: European Union. Accessed on: May 21, 2024.

FARD, Anahita Asgari. **E-commerce Law And Cybersecurity In Iran:** Nowadays, businesses are delegating more and more of their operations to the online arena, while the advertising and marketing activities are now predominantly conducted online, particularly on social networks. Mondaq, March 10, 2023. Available at: Mondaq. Accessed on: May 27, 2024.

FENG, Jenny. **Government-backed and infrastructure-oriented: The Chinese way of innovation.** Suzhou: The China Project, March 28, 2023. Available at: The China Project. Accessed on: May 26, 2024.

FINANCECHARTS. **Biggest Companies in the World by Market Cap for May 2024**. FinanceCharts.com, 2024. Available at: Financecharts. Accessed on: May 26, 2024.

FLASHPOINT INTEL TEAM. **Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way**. Washington, DC: FLASHPOINT.com. Available at: Flashpoint Intel Team. Accessed on: May 19, 2024.

FOLHA DE SÃO PAULO. Brazilian Electoral Court Regulates Artificial Intelligence in Elections and Prohibits Deepfake Use by Campaigns. Available at: Folha de São Paulo. Accessed on: May 21, 2024.

FORBES. #1741 Eugene Kaspersky. New Jersey: Forbes, April 4, 2024. Available at: Forbes. Accessed on: May 15, 2024.

FRASSON-QUENOZ, Florent; GONZÁLEZ, César Augusto Niño. Colombia's Cybersecurity Predicament: State making, strategic challenges, and cyberspace. In: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 42, pp. 494-503.

FRAUNHOFER-GESELLSCHAFT. **Fraunhofer-Gesellschaft**. Available at: FRAUNHOFER-GESELLSCHAFT. Accessed on: May 23, 2024.

GALAL, Saifaddin. **Internet usage in Africa - statistics & facts.** Statista, January 19, 2024. Available at: Statista. Accessed on: May 31, 2024.

GALAL, Saifaddin. **Number of internet users in Africa as of January 2024, by country (in millions).** Statista, 2024. Available at: Statista. Accessed on: May 19, 2024.

GILBERT, Ben. **The biggest game company in the world isn't Nintendo — it's a Chinese company that has a piece of everything from 'Fortnite' to 'League of Legends'**. New York: Business Insider, October 2019. Available at: Business Insider. Accessed on: May 27, 2024.

GILES, Keir. **Russia and cyber security. In:** Nação e Defesa. 2012, n.º 133, 5.ª ed. p. 69-88. Available at: Repositório Comum. Accessed on: May 19, 2024.

GLOBAL CYBER SECURITY CAPACITY CENTER. **Cyber Security Capacity Review.** Available at: Global Security Capacity Center. Accessed on: May 21, 2024.

GLOBAL INITIATIVE AGAINST ORGANIZED CRIME. **Monitoring illicit arms flows from the conflict in Ukraine.** Available at: Global Initiative Against Organized Crime. Accessed on: May 27, 2024.

GLOBAL INITIATIVE AGAINST ORGANIZED CRIME. **The Organized Crime Index**. Germany. Available at: Global Initiative Against Organized Crime. Accessed on: May 23, 2024.

GOEL, V.; PERLROTH, N. **Yahoo Says 1 Billion User Accounts Were Hacked**. The New York Times, 14 dez. 2016. Available at: The NY Times. Accessed on: May 31, 2024.

GOODIN, Dan. Kaspersky: Yes, we obtained NSA secrets. No, we didn't help steal them. Ars Technica. Available at: ARS Technica. Accessed on: May 19, 2024.

GOOGLE. **Google Cybersecurity Certificate**. GOOGLE, 2023. Available at: GOOGLE. Accessed on: May 27, 2024.

GOOGLE. **Google Cybersecurity Innovations**. GOOGLE, 2023. Available at: GOOGLE. Accessed on: May 27, 2024.

GOOGLE. **Growth Academy: AI for Cybersecurity**. GOOGLE, 2023. Available at: GOOGLE. Accessed on: May 28, 2024.

GOV.BR. **Brazil will use data science and A.I. to bring together investments in science and technology projects.** Available at: GOV.BR. Accessed on: May 21, 2024.

GOV.BR. **Comitê Nacional de Cibersegurança.** Available at: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber. Accessed on: May 21, 2024.
GOVERNMENT OF PAKISTAN. **United Nations.** Available at: GOV.BR. Accessed on: May 27, 2024.

GRAHAM, Loren R. (2004) **Science in Russia and the Soviet Union. A Short History.** Series: Cambridge Studies in the History of Science. Cambridge: Cambridge University Press, February 26, 1993. ISBN 978-0-521-28789-0

GROSS, Michaell Joseph. **Silent War**. Vanity Fair, June 6, 2013. Available at: Vanity Fair. Accessed on: May 27, 2024.

GUILBERT, Kieran. **Webcam Slavery: Tech turns Filipino families into cybersex child traffickers.** Available at: Reuters. Accessed on: May 20, 2024.

GUPTA, Maanak et al. **From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy**. IEEE Access, vol. 11, 2023. Available at: IEEE Xplore. Accessed on: May 28, 2024.

HALLIDAY, Josh. **Stuxnet worm is the 'work of a national government agency'**. The Guardian, September 24, 2010. Available at: The Guardian. Accessed on: May 27, 2024.

HALPERN, Micah. **Iran Flexes Its Power by Transporting Turkey to the Stone Age**. Observer, April 22, 2015. Available at: Observer. Accessed on: May 27, 2024.

HELMHOLTZ-GEMEINSCHAFT DEUTSCHER FORSCHUNGSZENTREN. **Helmholtz Association**. Available at: Helmholtz. Accessed on: May 23, 2024.

HM GOVERNMENT. **National AI Strategy.** Available at:

HO, Mike. **The Four Great Inventions of Ancient China.** China: China Highlights, September 28, 2023. Available at: China Highlights. Accessed on: May 26, 2024.

HOSKINS, Peter; WANG, Fan. **WeChat: Why does Elon Musk want X to emulate China's everything-app?.** United Kingdom: BBC News, July 29, 2023. Available at: BBC News. Accessed on: May 29, 2024.

HUAWEI. **2023 Annual Report.** Shenzhen: Huawei, 2023. Available at: Huawei. Accessed on: May 26, 2024.

IASIELLO, Emilio. **Cyber Attack: A Dull Tool to Shape Foreign Policy**. Tallinn: NATO CCD COE Publications, 2013. Available at: CCDCOE. Accessed on: May 22, 2024.

ICLTC AUSTRALIA. **A new look at the Budapest Convention on Cybercrime**. Available at: ICLTC Australia. Accessed on: May 27, 2024.

INHOUSELAWYER. **Data protection and cybersecurity in Brazil.** Available at: INHOUSELAWYER. Accessed on: May 21, 2024.

INTERNATIONAL MONETARY FUND. **World Economic Database**. Available at: IMF. Accessed on: May 20, 2024.

INTERNATIONAL TELECOMMUNICATIONS UNION. **Global Cybersecurity Index**. International Telecommunications Union, 2020. Available at: ITU. Accessed on: May 27, 2024.

INTERPOL. **Fingerprints.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL and UN join forces to counter exploitation of the Internet for terrorist activities.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL Innovation Centre**. Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL's Contribution to the Comprehensive International Convention on Countering the Use of Information Communications Technologies for Criminal Purposes.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL's Proposal for the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL's Rules on the Processing of Data.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **INTERPOL-led operation targets growing cyber threats,** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **Online African organized crime from surface to dark web.** 2020. Available at: INTERPOL. Accessed on: May 20, 2024.

INTERPOL. **Our History.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **Our Partners.** Available at: INTERPOL. Accessed on: March 20, 2024.

INTERPOL. **Towards Responsible AI Innovation.** Available at: INTERPOL. Accessed on: March 20, 2024.

ISPANOVIC, Igor, et al. **Battle for Balkan Cybersecurity**: Threats and Implications of Biometrics and Digital Identity. Balkan Insight, June 30, 2023. Available at: Balkan Insight. Accessed on: May 27, 2024.

JACKSON, Camille Marie. **Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success**. New Voices in Public Policy, vol. 7, 2013. Available at: https://www.semanticscholar.org/paper/Estonian-Cyber-Policy-After-the-2007-Attacks%3A-of-Jackson/ed3b6ecf3be6b14ee588f89ed95d501405a3c0c5. Accessed on: May 22, 2024.

JIA, Denise; ZHANQUI, Ye. **China Outlines Ambitions to Become World Leader in AI by 2025.** Beijing: Caixin Global, July 21, 2017. Available at: Caixing Global. Accessed on: May 27, 2024.

JONES, Sam; ARNOLD, Martin. UK spymasters raise suspicions over Kaspersky software's Russia links. London: The Financial Times, November 12, 2017. Available at: The Financial Times. Accessed on: May 19, 2024.

KASPERSKY LAB. **About**. Moscow: Kaspersky. Available at: Kaspersky Lab. Accessed on: May 20, 2024.

KASPERSKY LAB. Kaspersky completes its data-processing relocation to Switzerland and opens new Transparency Center in North America. Moscow: November 17, 2020. Available at: Kaspersky Lab. Accessed on: May 20, 2024.

KASPERSKY LAB. Transparency. Moscow: 2024. Available at: Kaspersky Lab. Accessed on: May 20, 2024.

KASPERSKY. **Brazil Banks in the Malware Glare**. Available at: YouTube. Accessed on: May 21, 2024.

KIRKPATRICK, David. The Facebook Effect: The Inside Story of the Company That Is Connecting the World. New York: Simon & Schuster. Published on June 8, 2010. pp. 20–21. ISBN 978-1-4391-0211-4. Archived from the original on November 12, 2012.

KO, June. **The Chinese government used technology to get a grip on coronavirus – and take control of its people.** Hong Kong: The Independent, April 14, 2020. Available at: The Independent. Accessed on: May 27, 2024.

KOBEK, Luisa Parraguez. **The State of Cybersecurity in Mexico: An Overview**. Wilson Center, Washington, DC, 2017. Available at: Wilson Center. Accessed on: May 26, 2024.

KOBEK, Luisa Parraguez; CALDERA, Erick. **Cyber Security and Habeas Data: The Latin American Response to information Security and Data Protection**. Revista Oasis, no. 24, pp. 109-128, Bogotá, 2016. Available at: Revista Oasis. Accessed on: May 26, 2024.

KRAMER, Andrew E.; PERLROTH, Nicole. Expert Issues a Cyberwar Warning. New York: The New York Times, June 3, 2012. Available at: The NY Times. Accessed on: May 17, 2024.

LAWRENCE, D. **Tor Anonymity Software vs. the National Security Agency - Businessweek**. Available at: Web Archive. Accessed on: May 31, 2024.

LEIBNIZ-GEMEINSCHAFT. **Leibniz Association**. Available at: Leibniz-Gemeinschaft. Accessed on: May 23, 2024.

LEVINE, Y. **Almost everyone involved in developing Tor was (or is) funded by the US government**. Available at: Pando. Accessed on: May 31, 2024.

LEWIS, James Andrew. **Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States**. Inter-American Development Bank, 2016. Available at: IADB. Accessed on: May 22, 2024.

LICHTER, Eyal. **Cybersecurity in Israel**: statistics & facts. Statista, December 21, 2023. Available at: Statista. Accessed on: May 27, 2024.

LICHTER, Eyal. **Share of cybercrime incidents among individuals in Israel in 2021, by type**. Statista, March 26, 2024. Available at: Statista. Accessed on: May 27, 2024.

LITVINENKO, Alexander; FELSHTINSKY, Yuri. **Blowing up Russia:** terror from within. Vol 1. Rússia: S.P.I. Books, 2002.

LUBOLD, Gordon; HARRIS, Shane. **Russian Hackers Stole NSA Data on U.S. Cyber Defense.** New York: Wall Street Journal, October 5, 2017. Available at: The Wall Street Journal. Accessed on: May 16, 2024.

LUO, Dora; WANG, Yanchen. **China - Data Protection Overview.** Beijing: OneTrust DataGuidance, October, 2023. Available at: Data Guidance. Accessed on: May 27, 2024.

MACASKILL, Ewen. **Iran to blame for cyber-attack on MPs' emails – British intelligence**. The Guardian, October 14 , 2017. Available at: The Guardian. Accessed on: May 27, 2024.

MAGID, Jacob; HOROVITZ, Michael. **Albania Cuts Diplomatic Ties With Iran, Boots Out Diplomats Over July Cyberattack**. The Times of Israel, September 7, 2022. Available at: The Times of Israel. Accessed on: May 27, 2024.

MARI, ANGELICA. **Brazil Is The World's Second Most Vulnerable Country To Cyberattacks.** Available at: Forbes. Accessed on: May 21, 2024.

MARI, ANGELICA.**Brazil Among Most Optimistic Countries About AI, Study Says.** Available at: Forbes. Accessed on: May 21, 2024.

MASSACHUSETTS Institue of Technology #2 Best Global Universities. Available at: US NEWS. Accessed on: May 31, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **1.1 Mission and Objectives | Policies**. Available at: MIT. Accessed on: June 1, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **12.1 Relations with Government and Community | Policies**. Available at: MIT. Accessed on: June 1, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About | MIT Lincoln Laboratory**. Available at: MIT. Accessed on: May 31, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **About MIT | MIT - Massachusetts Institute of Technology**. Available at: MIT. Accessed on: May 31, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Applied Cybersecurity | Professional Education**. Available at: MIT. Accessed on: June 1, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Computer Science – MIT EECS**. Available at: https://www.eecs.mit.edu/research/computer-science/. Accessed on: June 1, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **Cyber Security and Information Sciences | MIT Lincoln Laboratory**. Available at: MIT. Accessed on: May 31, 2024.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. **MIT Partners**. Available at: MIT. Accessed on: June 1, 2024

MATAMIS, J. **False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War • Stimson Center**. Available at: Stimson Center. Accessed on: May 27, 2024.

MATLACK, Carol. **The Company Securing Your Internet Has Close Ties to Russian Spies.** Germany: Bloomberg.com. Archived from the original on 2015-03-20. Available at: Bloomberg. Accessed on: May 20, 2024.

MATLACK, Carol. The Company Securing Your Internet Has Close Ties to Russian Spies. Germany: Bloomberg, March 20, 2015. Germany. Available at: Bloomberg. Accessed on: May 20, 2024.

MATTOS FILHO. **Artificial intelligence in Brazilian health and supplementary health services.** Available at: Mattos Filho. Accessed on: May 21, 2024.

MATTOS FILHO. **Decree establishing Brazil's National Cybersecurity Policy enacted**. Available at: Mattos Filho. Accessed on: May 21, 2021.

MAX-PLANCK-GESELLSCHAFT. **Max Planck Society: Homepage.** Available at: Max Plank Society. Accessed on: May 23, 2024.

MEENAGH, Brian A.; TUCKER, Lucy. **Six Months Until Enforcement**: Key Compliance Steps for Saudi Arabia's Data Protection Law. Global Privacy & Security Compliance Law Blog, March 13, 2024. Available at: Global Privacy & Security. Accessed on: May 27, 2024.

MÉNDEZ, Júlio César Villanueva. **La ciberdefensa en Colombia**. Institutional Repository Universidad Piloto de Colombia, Bogotá, 2015. Available at: Repository Unipiloto. Accessed on: May 26, 2024.

META PLATFORMS, INC. California: January 4, 2004. Available at: Meta. Accessed on: May 20,2024.

META PLATFORMS, INC. California: January 4, 2004. Available at: Meta. Accessed on: May 20, 2024.

MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION. **The world leader of black transplants: in Ukraine, organs are traded online and offline**, “Rossiiskaya Gazeta”, August 7, 2023. Available at: Ministry of Foreign Affairs of the Russian Federation. Accessed on: May 27, 2024.

MINISTRY OF SCIENCE AND TECHNOLOGY OF THE PEOPLE'S REPUBLIC OF CHINA. **National High-tech R&D Program (863 Program).** Beijing: Ministry of Science and Technology of the People's Republic of China. Available at: Ministry of Science and Technology of the People's Republic of China. Accessed on: May 26, 2024.

MTHEMBU, Mpakwana Annastacia. High road in regulating online child pornography in South Africa. In: **Computer Law & Security Review.** South Africa: Elsevier Ltd, 2012. Vol. 28, 4 ed, 438-444. Available at: DOI Foundation. Accessed on: May 19, 2024.

MTUZE, Sizwe Snail ka. MUSONI, Melody. **An overview of cybercrime law in South Africa**. International Cybersecurity Law Review, 2023. Vol 4, 299–323. Available at: DOI Foundation. Accessed on: May 20, 2024.

MUGGAH, ROBERT. **Bolsonaro Is Already Undermining Brazil’s Upcoming Election.** Available at: Foreign Policy. Accessed on: May 21, 2024.

NAKASHIMA, Ellen; GILLUM, Jack. U.S. bans use of Kaspersky software in federal agencies amid concerns of Russian espionage. Washington, DC: The Washington Post, September 13, 2017. Available at: The Washington Post. Accessed on: May 16, 2024.

NAST, C. **“Gay Furry Hackers” Breached a Nuclear Lab to Demand Catgirl Research**. Available at: https: Them. Accessed on: May 30, 2024.

NATIONAL BUREAU OF STATISTICS. **Research and Development Statistics.** Available at: Nigerian Bureau of Statistics. Accessed on: May 23, 2024.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA). **Research and Development Department.** Available at: NITDA. Accessed on: May 23, 2024.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **National Center For Artificial Intelligence and Robotics.** Available at: NITDA. Accessed on: May 23, 2024.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **National Information Technology Development Agency Act 2007**. Available at: NITDA. Edition1.pdf. Accessed on: May 23, 2024.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY. **Research and Development Department.** Available at: NITDA. Accessed on: May 23, 2024.

NICHOLSON, Craig. **R&D in Africa: 'We need to invest more'.** Durban: Research Professional News, June 2023. Available at: Research Professional News. Accessed on: May 20, 2024.

NINDL, Elisabeth. et al. **The 2023 EU Industrial R&D Investment Scoreboard.** Luxembourg: Publications Office of the European Union, 2023. Available at: DOI Foundation. Accessed on: May 27, 2024.

NINDL, Elisabeth. et al. **The 2023 EU Industrial R&D Investment Scoreboard.** Luxembourg: Publications Office of the European Union, 2023. Available at: DOI Foundation. Accessed on: May 26, 2024.

OCTOPUS CYBERCRIME COMMUNITY. **Pakistan Cybercrime Policies and Strategies.** Available at: Octopus Cybercrime Community. Accessed on: May 27, 2024.

OPARA, Emmanuel. **Cloud-based machine learning and sentiment analysis**. Georgia Southern University, Statesboro, USA, 2022. Available at: Digital Commons. Accessed on: May 26, 2024.

OPEN AI. **Disrupting malicious uses of AI by state-affiliated threat actors:** We terminated accounts associated with state-affiliated threat actors. Our findings show our models offer only limited, incremental capabilities for malicious cybersecurity tasks. OpenAi, February 14, 2024. Available at: Open AI. Accessed on: May 27, 2024.

OVERHAUL. **What Ukraine's weapons black market means for supply chains**. Available at: Overhaul. Accessed on: May 27, 2024.

PACETE, LUIZ GUSTAVO. **Por que 2023 será o ano da inteligência artificial?**. Available at: Forbes. Accessed on: May 21, 2024.

PAGBRASIL. **The State of Generative AI in Brazil.** Available at: PAGBRASIL. Accessed on: May 21, 2024.

PAPASPIROU, Vasilis et al. **Cybersecurity Revisited: Honeytokens meet Google Authenticator**. 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 2022. Available at: IEEE Xplore. Accessed on: March 28, 2024.

PARKER, J. **Ukraine mobile network Kyivstar hit by "cyber-attack"**. BBC News, December 12, 2023. Available at: BBC. Accessed on: May 27, 2024.

PERLROTH, Nicole; SANGER, David E. U.S. Embedded Spyware Overseas, Report Claims. New York: The New York Times, February 3, 2015. Available at: The NY Times. Accessed on: May 15, 2024.

PERMANENT MISSION OF THAILAND TO THE UNITED NATIONS. **Thailand Candidature for UNSC.** Available at: Permanent Mission of Thailand to the United Nations. Accessed on: May 27, 2024.

PETKAUSKAS, Vilius. Fears of Russian spying prompts Germany to ditch Kaspersky. CyberNews, March 21, 2022. Available at: Cyber News. Accessed on: May 19, 2024.

PETROSYAN, A. **U.S. government and cybercrime - Statistics & Facts**. Available at: Statista. Accessed on: May 31, 2024.

POLICE SERVICE OF NORTHERN IRELAND. **Cyber Protect.** Available at: Police Service of Northern Ireland.
Accessed on: May 21, 2024.

PRATT, M. **The 10 biggest ransomware attacks in history | TechTarget**. Available at: Tech Target. Accessed on: May 31, 2024.

PRIISALU, Jaan; OTTIS, Rain. **Personal control of privacy and data: Estonian experience**. Health Technol, vol. 7, pp. 441-451, 2017. Available at: Springer Link. Accessed on: May 22, 2024.

PWC. **A comparison of cybersecurity regulations: India.** Available at: PWC. Accessed on: May 23, 2024.

QS WORLD University Rankings for Computer Science and Information Systems 2023. Available at: QS Top Universities. Accessed on: May 31, 2024.

RASKA, MIchael. **Scientific Innovation and China's Military Modernization.** Singapore: The Diplomat, September 3, 2023. Available at: The Diplomat. Accessed on: May 26, 2024.

RAWAL, Bharat; EBERHARDT, Gabrielle; LEE, Jaein. **Cybersecurity Snapshot: Google, Twitter, and Other Online Databases**. Journal of Advanced Computer Science & Technology, vol. 5, no. 1, pp. 14-22, Amman, Jordan, 2016. Available at: Science Pubco. Accessed on: May 28, 2024.

REGIONAL ORGANISED CRIME UNIT. **Cyber Protect.** Available at: South East Cyber. Accessed on: May 21, 2024.

REPUBLIC OF SOUTH AFRICA. **Act No. 19 of 2020: Cybercrimes Act, 2020.** Cape Town: Government Gazette, 1 June 2021. Available at: Republic of South Africa. Accessed on: May 19, 2024.

REPUBLIC OF SOUTH AFRICA. **SA records an increase in research and development expenditure after COVID-19.** South Africa: South African Government News Agency, January 2024. Available at: Republic of South Africa. Accessed on: May 20, 2024.

REPUBLIC OF SOUTH AFRICA. **Survey shows that high proportion of R&D funding comes from government.** South Africa: South African Government News Agency, 2023. Available at: Republic of South Africa. Accessed on: May 20, 2024.

REUTERS. **Dutch government to phase out use of Kaspersky anti-virus software**. London: May 14, 2018. Available at: Reuters. Accessed on: May 19, 2024.

REUTERS. **Huawei to raise minimum annual R&D spending to at least US$15 billion.** Hong Kong: South China Morning Post, July 26, 2018. Available at: Reuters. Accessed on: May 26, 2024.

REUTERS. **Lithuania bans Kaspersky Lab software on sensitive computers**. London: December 21, 2017. Available at: Reuters. Accessed on: May 18, 2024.

REUTHERS, Thomson. **Russia responsible for killing of Alexander Litvinenko, European rights court rules.** CBC News, 2021. Available at: CBC. Accessed on: May 20, 2024.

ROBINSON, Nick; HARDY, Alex. Estonia: from the “Bronze Night” to cybersecurity pioneers. In: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 19, pp. 211-225.

RODRIGUEZ-HERNANDEZ, Saúl Mauricio; VELÁSQUEZ, Nicolás. Mexico and cybersecurity: policies, challenges, and concerns. In: ROMANIUK, Scott; MANJIKIAN, Mary. **Routledge Companion to Global Cyber-Security Strategy Book**. Abingdon, United Kingdom: Routledge, 2021. Chapter 41, pp. 484-493.

RUAN, Lotus. **What Does China’s New Cybersecurity Law Mean for Chinese Internet Companies?**. Arlington: The Diplomat, November 10, 2016. Available at: The Diplomat. Accessed on: May 27, 2024.

RUSSIA. **Ministry of internal affairs of the Russian Federation.** Acting minister status. Available at: http://government.ru/en/department/86/events/. Accessed on: May 20, 2024.

RUSSIAN FEDERATION. **Russian Federation Federal Law No. 40-FZ. Adopted by the State Duma 22 February 1995.** Archived 16 August 2018 at the Wayback Machine. Available at: Russian Law Consultant. Accessed on: May 21, 2024.

RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. WeChat privacy concerns and data collection. In: RYAN, Fergus; FRITZ, Audrey; IMPIOMBATO, Daria. **TikTok and WeChat: Curating and controlling global information flows.** Australia: Australian Strategic Institute, September 1, 2020. p. 43-46. Available at: JSTOR. Accessed on: May 27, 2024.

SA INTERNET growth accelerates. South Africa. World Wide Worx, 2010. Available at: World Wide Worx. Accessed on: May 20, 2024.

SALMA, Dita Aulia; MUNABARI, Fahlesa. **Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia**. Deviance Jurnal Kriminologi, vol. 7, pp. 32-45, Bekasi, Indonesia, 2023. Available at: Jornal Budiluhur. Accessed on: May 22, 2024.

SAMUIFORSALE. **Computer Crime Act Criminal Law.** Available at: SAMUIFORSALE. Accessed on: May 27, 2024.

SAUDI GAZETTE. **Follow basic cyber security standards, govt agencies told**. Saudi Gazette, October 07, 2018. Available at: Saudi Gazette. Accessed on: May 27, 2024.

SCHMITT, Michael. **Tallinn Manual on the International Law Applicable to Cyber Warfare**: prepared by the International Group of Experts as the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

SCHNEIDER, Eberhard. The Russian Federal Security Service under President Putin. In: **White, S. (eds) Politics and the Ruling Group in Putin's Russia**. Studies in Central and Eastern Europe. Palgrave Macmillan, London. DOI Foundation. Accessed on: May 21, 2024.

SECURITY REPORT. **Análise laboratorial indica alta nas atividades cibernéticas contra aliados de Israel**. Security Leaders, November 3, 2023. Available at: Security Leaders. Accessed on: May 27, 2024.

SECURITY SERVICE OF UKRAINE. **Cyber Security Situation Centre**. Available at: Security Service of Ukraine. Accessed on: May 27, 2024.

SHACHTMAN, Noah. Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals. San Francisco: WIRED. San Francisco, April 19, 2011. Available at: Wired. Accessed on: May 19, 2024.

SHAHEEN, Jeanne (2017-09-04). **The Russian Company That Is a Danger to Our Security**. New York: The New York Times, September 4, 2017. ISSN 0362-4331.

SHELLEY, Louise I. **Dark commerce: how a new illicit economy is threatening our future.** Princeton: Princeton University Press, 2018.

STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA. **China's R&D expenditure exceeds 3.3 trln yuan in 2023: minister.** Beijing: The State Council The People's Republic of China, March 5, 2024. Available at: State Council People's Republic of China. Accessed on: May 26, 2024.

STATISTA RESEARCH DEPARTENT. **Share of GDP expenditure on research and development in Russia from 2001 to 2020. Statista, February 17, 2023.** Available at: Statista. Accessed on: May 21, 2024.

STATISTA RESEARCH DEPARTMENT. **Worldwide Endpoint Security Revenue by Vendor, 2010.** Statista, September 2021. Available at: Statista. Accessed on: May 21, 2024.

STRETCH, B. **J. United States of America v. Dmitry Dokuchaev, Igor Sushchin, Alexey Belan, and Karim Baratov**, 28 fev. 2017. Available at: United States of America. Accessed on: May 31, 2024.

SUMEDHA, GUPTA. **Child Pornography and Internet Subcultures in India - a Legal Perspective.** Available at: Research Gate. Accessed on May 23, 2024.

SURFSHARK. **Cybercrime statistics.** 2022. Available at: Surfshark. Accessed on: May 20, 2024.

TENCENT GAMES. **Introduce**. Shenzhen: 2024. Available at: Tencent. Accessed on: May 27, 2024.

TENCENT. **#TencentInnovates: 8 Ways Tencent is Innovating to Make a Difference for People.** Shenzhen: Tencent, July 26, 2023. Available at: Tencent. Accessed on: May 26, 2024.

TENCENT. **About us**. Shenzhen: 2024. Available at: Tencent. Accessed on: May 27, 2024.

TENCENT. **Weixin's Palm Scan Payments Is Like Waving at a Friend.** Shenzhen: Tencent, 2024. Available at: Tencent. Accessed on: May 27, 2024.

TEXTOR, C. **Total expenditure on research and development (R&D) in China from 2013 to 2023.** Statista, May 24, 2024. Available at: Statista. Accessed on: May 26, 2024.

THE ALAN TURING INSTITUTE. **Understanding artificial intelligence ethics and safety.** Available at: The Alan Turing Institute. Accessed on: May 21, 2024.

THE COMMONWEALTH. **United Kingdom.** Available at: The Commonwealth. Accessed on: May 21, 2024.

THE CROWN PROSECUTION SERVICE. **Cybercrime - prosecution guidance.** Available at: The Crown Prosecution Service. Accessed on: May 21, 2024.

THE ECONOMIST. **Land of milk and start-ups.** Available at: The Economist. Accessed on: May 31, 2024.

THE ECONOMIST. **Why is Brazil a hotspot for financial crime?.** Available at: The Economist. Accessed on: May 21, 2024.

THE GUARDIAN. **Turkey officially changes name at UN to Türkiye.** Available at: The Guardian. Accessed on: May 25, 2024.

THE INFOGRAPHICS SHOW. **How Russia is Attacking Ukraine With the Dark Web**. Available at: YouTube. Accessed on: May 29, 2024.

THE MINISTRY OF COMMUNICATION TECHNOLOGY. **National Information and Communication Technology (ICT) Policy**. Available at: NITDA. Accessed on: May 24, 2024.

THE NATIONAL. **Cybercrime in Brazil.** Available at: YouTube. Accessed on: May 21, 2024.

THE ORGANIZED CRIME INDEX. **Nigeria**. Available at: Ocindex. Accessed on: May 24, 2024.

THE RECORD. **Interpol arrests more than 30 cybercriminals in global 'Synergia' operation.** Available at: The Record. Accessed on: March 20, 2024.

THE WHITE HOUSE. **Prosperity, Security, and Openness in a Networked World**. Available at: The White House. Accessed on: May 31, 2024.

THE WORLD BANK. **China**. Washington, DC: The World Bank Group, 2024. Available at: The World Bank. Accessed on: May 27, 2024.

THOMALA, Lai Lin. **Number of monthly active WeChat users from 4th quarter 2013 to 4th quarter 2023**. Statista, April 8, 2024. Available at: Statista. Accessed on: May 29, 2024.

TIDY, J. **Why is it so rare to hear about Western cyber-attacks?** BBC News, 23 jun. 2023. Available at: BBC. Accessed on: May 31, 2024.

TRUMP, Donald J. **Executive Order on Addressing the Threat Posed by WeChat**. Washington DC: The White House, August 6, 2020. Available at: The White House. Accessed on: May 27, 2024.

UNCAC Signature and Ratification status. Available at: United Nations Office on Drugs and Crime. Accessed on: May 31, 2024.

UNITED KINGDOM RESEARCH AND DEVELOPMENT. **About UK Research and Innovation.** Available at: UKRI. Accessed on: May 21, 2024.

UNITED KINGDOM RESEARCH AND DEVELOPMENT. **Explainer: how UKRI's institutes support research and innovation.** Available at: UKRI. Accessed on: May 21, 2024.

UNITED KINGDOM. **£360 million to boost British manufacturing and R&D.** UK Government. Accessed on May 21, 2024.

UNITED KINGDOM. **Convention on cybercrime.** Available at: UK Government. Accessed on: May 21, 2024.

UNITED KINGDOM. **National Cyber Security Centre.** Available at: https://www.gov.uk/government/organisations/national-cyber-security-centre. Accessed on: May 21, 2024.

UNITED KINGDOM. **Review of the Computer Misuse Act 1990: consultation and response to call for information.** Available at: UK Government. Accessed on: May 21, 2024.

UNITED KINGDOM. **UK Research and Development.** Available at: UK Government. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **1st Statement - Turkish Mission to the UN.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 25, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **About the Liaison and Partnership Office in Brazil.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Brazilian Government's position regarding the objectives, scope and structure of an international convention on countering the use of information and communications technologies for criminal purposes.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profile**: Iran (Islamic Republic of). 2024. Available at: United Nations Office on Drugs and Crime. Accessed on: May 27, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profile**: Serbia. 2024. Available at: United Nations Office on Drugs and Crime. Accessed on: May 27, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles:** Germany. Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Country Profiles:** United Kingdom of Great Britain and Northern Ireland. Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Cybercrime reporting and prevention.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 25, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Global Report on Trafficking in Persons 2022.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **India:** UNODC initiative focuses on empowering families to protect young people from drugs and crime**.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **INTERPOL's General Statement.** Available at: United Nations Office on Drugs and Crime. Accessed on: March 20, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (New York, 15 November 2000).** Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Report of the United Nations Office on Drugs and Crime on the International Classification of Crime for Statistical Purposes.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 25, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Statement of the Republic of Turkey.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 25, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **The United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules)**. Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Turkey's Initial Views regarding the Scope, Objectives and Structure of an International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 25, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UK announces new financial contributions to support UNODC's anti-corruption work**. Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UK National Submission on the UN Cybercrime Treaty.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 21, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNCAC Signature and Ratification status.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 23, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **United Nations and Philippines Launch New Project to Support Victims of Terrorism Through Legislative Frameworks.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 18, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC in Ukraine Factsheet**. Available at: United Nations Office on Drugs and Crime. Accessed on: May 27, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC Programme Office in Ukraine**. Available at: United Nations Office on Drugs and Crime. Accessed on: May 27, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **UNODC-Russia Partnership on Counter-Narcotics Training for Central Asia, Afghanistan and Pakistan**

(Phase IV). September 13-17, 2021. Available at: United Nations Office on Drugs and Crime. Accessed on: May 20, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME.. **UNCAC Signature and Ratification status.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 18, 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME.. **United Nations Convention against Corruption.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 18, 2024.

UNITED NATIONS PHILIPPINES. **United Nations in the Philippines.** Available at: https://philippines.un.org/en/about/about-the-un. Accessed on: May 18, 2024.
UNITED NATIONS. **12. United Nations Convention against Transnational Organized Crime**. New York, 2000. Available at: United Nations Philippines. Accessed on: May 20, 2024.

UNITED NATIONS. **EU–Nigeria–UNODC–CTED Partnership Project to Counter Terrorism and Violent Extremism Closes**. Available at: United Nations. Accessed on: May 24, 2024.

UNITED NATIONS. **History of the United Nations.** Available at: United Nations. Accessed on May 21, 2024.

UNITED NATIONS. **Member States.** Available at: United Nations. Accessed on: May 19, 2024.

UNITED NATIONS. **Restoration of the lawful rights of the People's Republic of China in the United Nations.** UN: General Assembly, 1971. Available at: United Nations. Accessed on: 24 May 2024

UNITED NATIONS. **United Nations Office on Drugs and Crime to Open Office in Beijing.** Vienna: UN Information Service, 2005. Available at: United Nations. Accessed on: 24 May 2024.

UNITED NATIONS.**15. Single Convention on Narcotic Drugs, 1961.** New York, 1961. Available at: United Nations. Accessed on: May 20, 2024.

UNITED STATES OF AMERICA. **Securities and exchange commission, under the securities act of 1993. Registration statement.** Available at: United States of America. Accessed on: May 20,2024.

UNIVERSITY SYSTEM OF GEORGIA. **A Brief History of the Internet.** Available at: USG. Accessed on: March 30, 2024.

UNODC EN MÉXICO. **Quiénes somos**. Vienne: United Nations Office on Drugs and Crime, 2024. Available at: United Nations Office on Drugs and Crime. Accessed on: May 26, 2024.

UNODC OPIOID STRATEGY. **The Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribben**. Vienne: United Nations Office on Drugs and Crime, 2022. Available at: United Nations Office on Drugs and Crime. Accessed on: May 26, 2024.

UNODC REGIONAL OFFICE FOR SOUTHEAST ASIA AND THE PACIFIC. **Scams and trafficking for forced criminality: UNODC establishes an emergency response network to combat human trafficking in Southeast Asia.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 27, 2024.

UNODC REGIONAL OFFICE FOR SOUTHEAST ASIA AND THE PACIFIC. **The Philippines joins the UNODC-WCO Container Control Program.** Available at: United Nations Office on Drugs and Crime. Accessed on: May 18, 2024.

URI, J. **65 Years Ago: Sputnik Ushers in the Space Age - NASA.** Available at: NASA. Accessed on: March 30, 2024.

VICE NEWS. **Exposing the NSA's Mass Surveillance of Americans | CYBERWAR**. Available at: YouTube. Accessed on: May 30, 2024.

VICE NEWS. **The World's First Cyber Weapon Attack on a Nuclear Plant | Cyberwar**. Available at: YouTube. Accessed on: May 30, 2024.

VOLZ, Dustin; FITZGERALD, Drew; CHAMPELLI, Peter; BROWN, Emma. **U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships. Published by the Wall Street Journal, May 19, 2024.** Available at: Wall Street Journal. Accessed on: May 21, 2024.

VOX UKRAINE. **FAKE: Ukraine is the world leader in "black transplantology" article**. Available at: Vox Ukraine. Accessed on: May 27, 2024.

VYTOVTOV, A.E. **Revisiting the Concept of Economic Crimes in Russian Criminal Legislation.** Gaps in Russian Legislation, v.16, n4, p.374-378, august 2023. ISSN 2072-3164 (Print) ISSN 2310-7049 (Electronic).

WAGNER, Jack. **China's Cybersecurity Law: What You Need to Know.** Arlington: The Diplomat, June 01, 2017. Available at: The Diplomat. Accessed on: May 27, 2024.

WORDEN, R L; SAVADA, A M; DOLAN, R E. Science and Technology. In: WORDEN, R L; SAVADA, A M; DOLAN, R E. **China: A Country Study.** Washington, D.C.: Library of Congress, 1988. p. 371-406. Available at: Library of Congress. Accessed on: May 26, 2024.

WORLD ECONOMIC FORUM. **Innovative approaches for unlocking R&D funding in Africa.** November 9, 2023. Available at: World Economic Forum. on: May 31, 2024.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **Global Innovation Index: Innovation in the face of uncertainty.** Geneva: WIPO, 2024. Available at: WIPO. Accessed on: May 26, 2024.

WORLD POPULATION REVIEW. **London Population 2024.** Available at: World Population Review. Accessed on: May 21, 2024.

WORLDOMETER. **Germany Population (2024)**. Available at: Worldometer. Accessed on: May 23, 2024.

WORLDOMETER. **Nigeria Population (2024)**. Available at: Worldometer. Accessed on: May 23, 2024.

WORLDOMETER. **U.K. Population (2024).** Available at: Worldometer. Accessed on: May 21, 2024.

XINHUA. **China unveils Internet Plus action plan to fuel growth**. Beijing: The State Council of The People's Republic of China, July 4, 2025. Available at: XINHUA. Accessed on: May 27, 2024.

XINHUA. **China's internet giants report rapid Q3 growth amid innovation drive**. Beijing: Xinhua, November 24, 2023. Available at: XINHUA. Accessed on: May 26, 2024.

YANKOVSKI, A. **Key lessons from Ukraine's eight-year struggle against russian cyber warfare - KPMG Ukraine**. Available at: KPMG Ukraine. Accessed on: May 27, 2024.