

# CONNECTIONS

---

## THE QUARTERLY JOURNAL

CONNECTIONS SPECIAL ISSUE



PARTNERSHIP FOR  
PEACE CONSORTIUM  
OF DEFENSE  
ACADEMIES AND  
SECURITY STUDIES  
INSTITUTES

SPRING 2021

## COUNTERING CRIME AND DISINFORMATION IN CYBERSPACE

---

EDITORS:  
SEAN COSTIGAN AND TODOR TAGAREV

# *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*

## **The PfP Consortium Editorial Board**

Sean S. Costigan	Editor-In-Chief
Ed Clark	Managing Editor
Aida Alymbaeva	Institute for Analysis and Initiatives Development, Bishkek
Pal Dunay	George C. Marshall Center, Garmisch-Partenkirchen
Philipp Flury	Geneva Centre for Security Policy, Geneva
Piotr Gawliczek	University of Warmia and Mazury in Olsztyn, Poland
Hans-Joachim Giessmann	Berghof Conflict Research Centre, Berlin
Dinos Kerigan-Kyrou	Joint Command & Staff Course, Military College, Irish Defence Forces
Chris Pallaris	i-intelligence GmbH, Zurich
Tamara Pataraiia	Caucasian Institute for Peace, Democracy and Development
Todor Tagarev	Bulgarian Academy of Sciences, Sofia
Eneken Tikk	Cyber Policy Institute, Jyväskylä

The views expressed and articles appearing in all *Connections* publications are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

This edition is supported by the United States government. The Consortium's family of publications is available at no cost at <http://www.connections-qj.org>. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the Partnership for Peace Consortium at [PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org).

Dr. Raphael Perl  
Executive Director

Sean S. Costigan  
Editor-In-Chief and Chair, Editorial Board



ISSN 1812-1098, e-ISSN 1812-2973

# CONNECTIONS

## THE QUARTERLY JOURNAL

**Vol. 20, no. 2, Spring 2021**





**Contents**

## Vol. 20, no. 2, Spring 2021

### Editorial

- Countering Crime, Hate Speech, and Disinformation in Cyberspace 5  
*Sean S. Costigan and Todor Tagarev*

### Research Articles

- Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty 9  
*Sean S. Costigan*
- Evolution of Police Roles in Combatting Cybercrime in the Czech Republic, 2015-2020 15  
*Lukáš Vilím*
- Trusting ICT Providers – Can Corporate Cyber Confidence-Building Measures Help? 21  
*Matthias Klaus*
- Cyber Skills Gaps – A Systematic Review of the Academic Literature 33  
*Harri Ruoslahti, Janel Coburn, Amir Trent, and Ilkka Tikanmäki*
- Disinformation: Policy Responses to Building Citizen Resiliency 47  
*Inez Miyamoto*
- Social Media – Hate Speech – Hate Crime 57  
*Lukáš Vilím*

## Table of Contents

Corruption as a Cybersecurity Threat in the New World Order	75
<i>Bohdan M. Holovkin, Oleksii V. Tavalzhanskyi, and Oleksandr V. Lysodyed</i>	
Future Development of Quantum Computing and Its Relevance to NATO	89
<i>Rupert A. Brandmeier, Jörn-Alexander Heye, and Clemens Woywod</i>	



## Countering Crime, Hate Speech, and Disinformation in Cyberspace

*Sean S. Costigan*<sup>1</sup> and *Todor Tagarev*<sup>2</sup>

<sup>1</sup> *George C. Marshall European Center for Security Studies,*  
<https://www.marshallcenter.org/>

<sup>2</sup> *Institute of Information and Communication Technologies,*  
*Bulgarian Academy of Sciences, Sofia, Bulgaria,* <http://www.iict.bas.bg/EN>

**Abstract:** Increased connectivity and open access to the Internet provide malicious actors with novel opportunities for intelligence gathering, attacks on vulnerable targets, and shaping mass perceptions and behavior. In the editorial article to this edition of *Connections*, the issue editors review recent and emerging security-related challenges and responses. The focus is on the increase in cybercrime, corruption, the spread of hate speech, propaganda, and disinformation. In addition, the contributors elaborate on prospective solutions such as strengthening the legal regimes, including international norms, instituting confidence-building measures, and enhancing cyber skills, as well as the challenges for defense posed by the advances in quantum computing.

**Keywords:** cybercrime, hate speech, disinformation, resilience, corruption, quantum computing.

Today, cyberspace is deeply challenged by a variety of largely political concerns. This new humanizing of cyberspace may seem fitting to some who fretted for years over a relative lack of high-level political interest in the world's only new "domain." With cyber now being the topic of the day, it is easy to forget that, however notional, cyber was considered too technical to be worthy of elite policy attention until suddenly it was red hot and everywhere. Yet, as cyber silently

built momentum and impacts loomed, people in the know understood that cyber was more than a technical issue and began building programs of study and fashioning a new realm of knowledge that was combinatorial and interdisciplinary by nature. Just as there could be no cyber without technology, there was no way to do cyber without people.

This issue of *Connections* is a case in point. It brings to the readers' attention eight original articles presenting novel challenges that go beyond state-sponsored cyber operations<sup>1</sup> and look into cybercrime, corruption, dissemination of hate speech, propaganda, and disinformation in cyberspace, as well solutions from the realms of technology, policy-making, legislation, education and training.

Whether it is a consideration of how trust is developed between private companies<sup>2</sup> and people in cyberspace or the emerging developments and likely impacts of quantum computing,<sup>3</sup> we are entering a unique time for the study of cybersecurity. Technology will continue its march, in many cases driving new challenges to the surface, but mature policy and scholarship, such as what we see in this issue, will help situate change and create resilience. Technology and policy are joined at the hip. Cybersecurity is no longer a necessarily but largely insufficient technical pursuit designed to make products safer. It is a wholly mature field with dozens of interrelated, equally critical fields of inquiry.

As challenges mount, people and their awareness and skills become ever more critical.<sup>4</sup> Each advancing year the global population becomes increasingly dependent on cyberspace and a measure of cybersecurity. Some political systems have become ever more fearful of the power of cyberspace, betting on more complex systems and networks to control their citizens' perceptions<sup>5</sup> and

---

<sup>1</sup> Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," 12th International Conference on Cyber Conflict, CyCon 2020, online, May 26-29, 2020, pp. 129-155, <https://doi.org/10.23919/CyCon49761.2020.9131723>.

<sup>2</sup> Matthias Klaus, "Trusting ICT Providers – Can Corporate Cyber Confidence-Building Measures Help?" *Connections: The Quarterly Journal* 20, no. 2 (2021): 21-31, <https://doi.org/10.11610/Connections.20.2.03>.

<sup>3</sup> Rupert A. Brandmeier, Jörn-Alexander Heye, and Clemens Woywod, "Future Development of Quantum Computing and Its Relevance to NATO," *Connections: The Quarterly Journal* 20, no. 2 (2021): 89-110, <https://doi.org/10.11610/Connections.20.2.08>.

<sup>4</sup> Harri Ruoslahti, Janel Coburn, Amir Trent, and Ilkka Tikanmäki, "Cyber Skills Gaps – A Systematic Literature Review of Academic Literature," *Connections: The Quarterly Journal* 20, no. 2 (2021): 32-44, <https://doi.org/10.11610/Connections.20.2.04>.

<sup>5</sup> Martti J. Kari and Katri Pynnöniemi, "Theory of Strategic Culture: An analytical Framework for Russian Cyber Threat Perception," *Journal of Strategic Studies* (in press), <https://doi.org/10.1080/01402390.2019.1663411>.



shape their behavior and political destiny. Decoupling from the Internet has become a goal for too many states.<sup>6</sup> Disinformation campaigns move across borders and target individuals with precision, putting individual resiliency and critical thinking to the test.<sup>7</sup> Research in this issue shows just how important cyber skills are for the functioning of society.

Democratized tools and knowledge mean that cybercriminals can now have the same power as states or large corporations. What were once small-time operations are very often now criminal cartels, some even running crime as a service, while police and authorities come to grips with the new face of cybercrime.<sup>8</sup> States are also using the new threat of cybercrime to justify radically different visions of cyberspace.

In the meantime, global workforce challenges hamper our collective ability to secure cyberspace and improve the infrastructure on which we rely.<sup>9</sup> To meet the need, cybersecurity programs must do their utmost to graduate experts with knowledge of all facets of cyber: people, process, and technology.

This issue of *Connections* is dedicated to all the hard-working cybersecurity experts out there. We are grateful for your dedication and sense of mission.

Finally, a great measure of thanks goes to the authors of this issue and their patience as this excellent issue finally comes together.

## Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

---

<sup>6</sup> Rongbin Han and Li Shao, "Scaling Authoritarian Information Control: How China Adjusts the Level of Online Censorship," *Political Research Quarterly* (in press), <https://doi.org/10.1177/10659129211064536>.

<sup>7</sup> Inez Miyamoto, "Disinformation: Policy Responses to Building Citizen Resiliency," *Connections: The Quarterly Journal* 20, no. 2 (2021): 45-53, <https://doi.org/10.11610/Connections.20.2.05>.

<sup>8</sup> Lukáš Vilím, "The Issue of Combating Cybercrime in the Czech Republic with Regard to the Last Five Years," *Connections: The Quarterly Journal* 20, no. 2 (2021): 15-20, <https://doi.org/10.11610/Connections.20.2.02>.

<sup>9</sup> Daniel Hulatt and Eliana Stavrou, "The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation," in *Human Aspects of Information Security and Assurance*, edited by Steven Furnell and Nathan Clarke, *IFIP Advances in Information and Communication Technology*, vol. 613 (Cham: Springer, 2021), pp. 138-147, [https://doi.org/10.1007/978-3-030-81111-2\\_12](https://doi.org/10.1007/978-3-030-81111-2_12).

### About the Authors

**Sean S. Costigan** is a Professor at George C. Marshall European Center for Security Studies and Senior Advisor to the Emerging Security Challenges working group of the Partnership for Peace Consortium.

E-mail: [sean.costigan@marshallcenter.org](mailto:sean.costigan@marshallcenter.org)

**Todor Tagarev** is an experienced security and defense policymaker with a background in cybernetics and control theory and applications. He is currently a professor at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and leads its Centre for Security and Defence Management. Prof. Tagarev has been a member of the Editorial Board of *Connections: The Quarterly Journal* since 2004. <https://orcid.org/0000-0003-4424-0201>



Sean S. Costigan, *Connections QJ* 20, no. 2 (2021): 9-13

<https://doi.org/10.11610/Connections.20.2.01>

Research Article

## Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty

*Sean S. Costigan*

*George C. Marshall European Center for Security Studies,*

<https://www.marshallcenter.org/>

**Abstract:** Under the guise of combating cybercrime, two radically different visions of cyberspace compete for attention on the international stage: a free-flowing model of cyberspace that democracies have championed is now challenged by a so-called sovereign model. Counter-democratic initiatives to reframe cyberspace in strictly national terms are underway with the likely result of decreased cooperation and increased risks of conflict and cybercrime.

**Keywords:** Cybercrime, Cyberspace, Sovereignty, Cooperation, Conflict

Global unrest is fast becoming the norm in cyberspace, where cybercriminals operate with relative impunity, and novel technologies allow nation-states to sharpen their practice of influence operations. There is a near-constant rate of hacks against computers – by one recent count every 39 seconds on average for devices connected to the Internet.<sup>1</sup> If cybercrime is not tackled, at risk is nothing less than trust in the government’s ability to deliver on the promise of security. 61% of Europeans worry that elections can be manipulated through cyberattacks. One in three Americans will find themselves a victim of some form of cybercrime this year alone, not to mention the risks of state interference.

Disinformation has consumed many news and policy cycles, no less now in the time of COVID-19. Russian disinformation campaigns have regularly pushed

---

<sup>1</sup> “Hackers Attack Every 39 Seconds,” *Security Magazine*, February 10, 2017, <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>.

out propaganda about the virus through think-tanks and suspect news services.<sup>2</sup> Cyberspace has emerged as a national security complex, affecting as it does governments, corporations, and individuals alike. Given this state of affairs, a universal cybercrime treaty would seem to benefit all.

Under the guise of combating cybercrime, two radically different visions of cyberspace compete for attention on the international stage. The first may be broadly characterized as a free-flowing model of cyberspace and has been championed by democracies. It is challenged by the second, the so-called “sovereign model,” where the primary focus is state control over information and, ultimately, people.

On 18 November 2019, a United Nations committee passed a Russia-backed cybercrime resolution by a vote of 88 to 58, with 34 countries abstaining. Russia’s successful vote set up an “Open-Ended Working Group” to examine cybercrime and methods to prevent it. While this development might sound potentially beneficial, it has direct consequences for the Budapest Convention on Cybercrime<sup>3</sup> and existing mechanisms for improving the fight against cybercrime, international and national legal efforts, as well as long-term foreign policy impacts in many areas beyond cyberspace.

The Budapest Convention is the only convention on cybercrime. However, it has come under sustained pressure from Russia and its foreign policy partners that argue its very existence is an effort to violate sovereignty. (Note that the Budapest Convention is open to the accession of countries that are not parties to the Council of Europe and is the means for international cooperation to tackle cybercrime.)

Russia has also been actively trying to physically move current discussions on cybercrime from their home in Vienna, Austria (where decisions are made through consensus) to New York, where a majority vote would seem to give Russia and China a significant advantage in the future proceedings.<sup>4</sup>

Moreover, Russia and China may parlay such wins at the United Nations to further not just their overarching goals of challenging the existence of universal human rights and the ideals of an open, free, and indivisible Internet, but also the post-World War II world order, which Russia currently, and China more principally, regards to primarily be a Western construction – and thus, in their conception, unjustly benefitting Western states.

---

<sup>2</sup> Julian E. Barnes and David E. Sanger, “Russian Intelligence Agencies Push Disinformation on Pandemic,” *The New York Times*, July 28, 2020, <https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>.

<sup>3</sup> Council of Europe, “Convention on Cybercrime,” Treaty No. 185, Budapest, November 23, 2001, [www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185).

<sup>4</sup> U.S. Department of State, “State Department Official on Multilateral Cyber Efforts,” Special Briefing, Office of the Spokesperson, Press Correspondents Room, December 19, 2019, <https://web.archive.org/web/20191220024014/https://www.state.gov/state-department-official-on-multilateral-cyber-efforts/>.

Considering these moves, this article argues that the West should prepare for future international negotiations that might not go according to plan, to include further gains by China and Russia to seek control over information and alter the course of cyberspace as we know it.

The Russian proposal for a global cybercrime convention as well as Russia's eagerness to further the "Open-ended Working Group on Developments in the Field of information and telecommunications in the context of international security"<sup>5</sup> are primarily political moves to strengthen the Russian goal of establishing "the system of international information security."<sup>6</sup> The system the Kremlin seeks to achieve would be based on a "Convention on International Information Security," with the United Nations and the International Telecommunications Union assigned to play major roles. Moreover, this Russian conception leans on strong, even absolute, state sovereignty, which undermines and overrides international obligations the state may have or be interpreted to have.<sup>7</sup>

Russian arguments for the purposes of a so-called sovereign internet (known as *RuNet*) stress several aspects of security by autonomy. The objective of a separate Russian internet was outlined in the 2017 information security doctrine<sup>8</sup> as "developing a national system of the Russian Internet segment management." The context of this ambition being "of ensuring information security in the field of strategic stability and equal strategic partnership" implicitly but effectively refers to the perceived information security threat from the United States. The purpose of the "national segment of the Internet," as it is also called, was to protect information as such and secure Russian critical infrastructure in the event of threats to the stability, security, and functional integrity.

Some Russians have come to justify the ostensible need to maintain Russian-to-Russian traffic within territorial borders through the use of financial arguments: by this reckoning, the cost of international routing may, in the future,

---

<sup>5</sup> United Nations Office for Disarmaments Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," <https://www.un.org/disarmament/ict-security/>.

<sup>6</sup> "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020," approved by the President of the Russian Federation on 24 July, 2013, accessed September 29, 2020, <http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russian-federation-in-the-field-of-international-information-security-to-2020.html>.

<sup>7</sup> Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet," *German Council on Foreign Relations*, January 16, 2020, <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>.

<sup>8</sup> *Doctrine of Information Security of the Russian Federation*, Approved by Decree of the President of the Russian Federation No. 646, December 5, 2016.

become too expensive.<sup>9</sup> The demand to pre-install Russian software to “track, filter, and reroute internet traffic”<sup>10</sup> can be read in the contexts of information security, critical infrastructure protection, and boosting national research and development markets.<sup>11</sup> Obviously, widening the coverage of federal (Roskomnadzor’s) enforcement mechanisms from routing traffic to all ITC devices also increases political and informational control over individuals.

It would appear then that these moves are intended to create a cloud of uncertainty that would undermine work done in the past and consensus regarding international norms in cyberspace while subverting the core values of an open, free and accessible Internet. Russia and China are working hand-in-hand to enforce what many experts maintain is a dystopian, state-control view of cyberspace on the world. This means exercising their authoritarian policies that are in stark contradiction with the democratic order and undercutting the framework of global economic order and business interests over the long term.

While the voting in the UN 3<sup>rd</sup> committee showed that there is no consensus to start negotiation or to establish a new legal instrument on cybercrime, it should be clear that this effort will not go away on its own. Furthermore, there is no consensus on the legal scope that such a new treaty on this issue should have. In addition, Western European nations appear to recognize that such a process would serve to divert efforts from national legislative reforms and current capacity building, essentially throwing a wrench into these efforts.

A new international legal instrument on cybercrime would duplicate existing work and preempt the conclusions of the open-ended intergovernmental UN expert group (IEG)<sup>12</sup> to conduct a comprehensive study of the problem of cybercrime and responses to it by member states.

Russia has not just maintained but has also developed and strengthened its call for an “international information security system.” Meanwhile, some experts argue that the West has not been particularly successful in its efforts to convince and engage states outside its perimeter.<sup>13</sup> Moscow and Beijing appear largely immune to name-and-shame strategies or accusations of cyberattacks and

---

<sup>9</sup> According to discussions with Kaspersky experts, currently only 2% of Russian-to-Russian traffic crosses its national borders.

<sup>10</sup> “Russia Internet: Law Introducing New Controls Comes into Force,” *BBC*, November 1, 2019, <https://www.bbc.com/news/world-europe-50259597>.

<sup>11</sup> For an opposite view see Alexandra Prokopenko, “Russia’s Sovereign Internet Law Will Destroy Innovation,” *The Moscow Times*, April 21, 2019, [www.themoscowtimes.com/2019/04/21/russias-sovereign-internet-law-will-destroy-innovation-a65317](http://www.themoscowtimes.com/2019/04/21/russias-sovereign-internet-law-will-destroy-innovation-a65317).

<sup>12</sup> The IEG is the main process at the level of the United Nations on the issue of cybercrime.

<sup>13</sup> Sally Adee, “The Global Internet Is Disintegrating: What Comes Next?” *BBC*, May 15, 2019, [www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next](http://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next).

espionage, such as with the SolarWinds breach.<sup>14</sup> Meanwhile, the authority of like-minded Western countries has been affected by leaks of foreign espionage,<sup>15</sup> news reports of mass surveillance,<sup>16</sup> weakening encryption,<sup>17</sup> and especially of government expectations of corporate assistance. To effectively push back on counter-democratic initiatives, the West needs to undermine one of the three pillars in the Kremlin's strategy: the general distrust towards ICTs, the insufficiency of existing international law, or the existential threat narrative. Another way to increase resilience in cyber discourse is to identify shared national interests and objectives across camps and continents, such as through the Framework for Responsible State Behavior in Cyberspace<sup>18</sup> and the Paris Call for Trust and Security in Cyberspace.<sup>19</sup> To advance, the West needs to prepare for treaty negotiations as one possible future. Preparing for that worst-case scenario, it should be possible to find new openings to avoid it.

## Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## About the Author

**Sean S. Costigan** – see the CV on page 8 of this issue, <https://doi.org/10.11610/Connections.20.2.00>

---

<sup>14</sup> Sean S. Costigan, "Charting a New Path for Cybersecurity after SolarWinds," *Diplomatic Courier*, January 4, 2021, [www.diplomaticcourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds](http://www.diplomaticcourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds).

<sup>15</sup> Patricia L. Bellia, "WikiLeaks and the Institutional Framework for National Security Disclosures," *Yale Law Journal* 121, no. 1448 (2012), April 2, 2012, Notre Dame Legal Studies Paper No. 12-59, <https://ssrn.com/abstract=2033207>.

<sup>16</sup> Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 2014): 121-144.

<sup>17</sup> Aaron Brantly, "Banning Encryption to Stop Terrorists: A Worse than Futile Exercise," *CTC Sentinel* 10, no. 7 (August 2017): 29-33, [https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel\\_Vol10Iss7-10.pdf](https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf).

<sup>18</sup> "Joint Statement on Advancing Responsible State Behavior in Cyberspace," United States Department of State, September 23, 2019, <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/> and "Eleven Norms of Responsible State Behaviour in Cyberspace," Federal Department of Foreign Affairs FDFA, April 7, 2021, <https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html>.

<sup>19</sup> "Paris Call for Trust and Security in Cyberspace – Paris Call," <https://pariscall.international/en/>.







Research Article

## Evolution of Police Roles in Combatting Cybercrime in the Czech Republic, 2015-2020

*Lukáš Vilím*

*Ministry of the Interior of the Czech Republic, <https://www.mvcr.cz/mvcren/>*

**Abstract:** The article reviews the expanding roles of the Police of the Czech Republic in countering cybercrime. The author emphasizes the importance of conceptual and strategic considerations underlying the emergence of new legislation, the financial support for purchasing new equipment, and the creation of new staff positions for professionals in cybercrime. Furthermore, it is of utmost importance to develop new strategies in line with the threats, challenges, and opportunities in cyberspace. Enhanced cooperation at all levels of the security system can facilitate the creation of strategies and thus make cyberspace a safer place.

**Keywords:** cybercrime, Budapest Convention, security system, strategy, contact point, critical information infrastructure.

A significant milestone in the fight against cybercrime in the Czech Republic is the Government's approval on July 10, 2017, of the "Concept for the Development of the Cybercrime Investigation Capabilities of the Police of the Czech Republic" (hereinafter the Concept) under number 502.

Of course, in this context, we cannot overlook the professionals who had been dealing with cybercrime earlier, whether at the local, regional, or national level. Certain changes in addressing this issue were already introduced in October 2015, when the Organized Crime Unit (*Útvar pro odhalování organizovaného zločinu – ÚOOZ*) began to deal intensively with cybercrime. In 2016, countering cybercrime became part of the conceptual program of the newly established nationwide unit of the National Organized Crime Agency (*Národní centrála proti organizovanému zločinu – NCOZ*). It must be noted as well that law enforcement authorities have paid attention to criminal activities in cyberspace since the launch of the Internet.

However, the Concept mentioned above was the first in the Czech Republic to address this issue comprehensively. It focused on various areas of action to strengthen significantly the ability of the Police of the Czech Republic to fight this type of crime – from the field of personnel reinforcement and education to legislative changes with impact across the entire Police of the Czech Republic. The text of the decision to adopt the Concept, also published on the website of the Czech Government, announced that the Concept

changed the organization and staffing of the Police of the Czech Republic from September 1, 2017. Thirty positions for members of the Police of the Czech Republic are added, with the respective increase of the budget for salaries of serving members of the security forces by CZK 4,595,280 in 2017. This decision will have a lasting effect for the subsequent years, with the implementation of the requirements for 2018 and the medium-term outlook for 2019 and 2020. The allocated budget will exceed the already approved limits for the Ministry of the Interior ... and 73 new positions will be added as of 2018.

The Concept set high demands for all those who participated in its implementation and worked to meet the requirements therein. Its advantage was in establishing a clear direction for detecting, documenting, and investigating this new kind of criminal activity. There has been a reinforcement of staff followed by a new system of education that should be able to train and educate police officers dealing with this specific issue at all levels.

In terms of legislation, Act No. 141/1961 Coll., On Criminal Procedure (Criminal Procedure Code) concerning the collection, storing, using, exchanging, and destroying of data was consequently amended. Attention was also paid to detecting, documenting, and investigating attacks on critical information infrastructure, including its protection against terrorist attacks, through amendments to Act No. 40/2009 Coll., The Criminal Code. More specifically, a new item (e) was added to the first paragraph of Article 311, thus adding severe attacks on computer systems essential for society and the state's operation (including important information systems and critical information infrastructure).

The importance of section 311 e) is in its focus on terrorist attacks in cyberspace and the related need to protect the constitutional system or the defense of the Czech Republic, as well as the basic political, economic or social structure, the citizens, and international organizations against political or extremist violence. A terrorist attack of this type can break the law by inserting data into a computer system or information rack or deleting or damaging data stored in a computer system (information rack) by reducing its quality or rendering it unusable. An attack against a computer system may affect the functioning of the state, the health of persons, the security, the economy, or the provision of the basic living needs of the population. Furthermore, an attack utilizing tailored

malware may impact a large number of computer systems and cause considerable damage.<sup>1</sup>

In 2019, the issue of expedited retention of data stored in a computer system or on an information carrier for the purposes of criminal proceedings was simplified when § 7b was added to the Criminal Procedure Code, allowing, under the fulfillment of specified conditions, to order a person to carry out expedited retention of data important for criminal proceedings. According to § 7b, data retention is a preliminary measure that provides the police authority with the necessary time to secure the data.<sup>2</sup>

Another relevant norm was introduced through amendment of Act No. 104/2013 Coll., On International Judicial Cooperation in Criminal Matters. A new § 65a enabled the provision of expedited transfer of data stored on a computer system located in the territory of a foreign state. This Act directly regulates the use of the relevant contact point for cybercrime of the Police of the Czech Republic to make data preservation requests abroad upon the consent of the Public Prosecutor's Office. Among the European member states, the stored data is requested through the European Investigation Order. Such request is issued or validated by the judicial authority in one EU country to allow the application of investigative measures to gather or use evidence in criminal matters carried out in another EU country. It is valid throughout the EU but does not apply in Denmark and Ireland.<sup>3</sup> Outside the European Union, data is requested through a Mutual Legal Assistance Treaty (MLAT) – an agreement between two or more countries to gather and exchange information in an effort to enforce public or criminal laws. A mutual legal assistance request is commonly used to formally interrogate a suspect in a criminal case when the suspect resides in a foreign country.<sup>4</sup>

A National Contact Point for Cybercrime was established to facilitate cooperation in an exemplary manner and thus fulfill the tasks arising for the Czech Republic from the Council of Europe Convention on Cybercrime (Convention on Cybercrime, Budapest, November 23, 2001, ETS No. 185). The necessary tasks are performed 24/7. This contact point also contributes significantly to the detection of cybercrime and is involved in saving lives in cases of suspected threats to life and health in cyberspace. The Czech National Contact Point for Cybercrime respects the following laws and conventions:

---

<sup>1</sup> Act No. 40/2009 Coll., "The Criminal Code of the Czech Republic," section 311, letter e).

<sup>2</sup> Act. No. 141/1961 Coll., "The Criminal Procedure of the Czech Republic."

<sup>3</sup> Eurojust, European Union Agency for Criminal Justice Cooperation, "European Investigation Order," accessed April 18, 2021, <https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/european-investigation-order-eio>.

<sup>4</sup> European Commission, "Mutual Legal Assistance and Extradition. Combating Crime Across Borders," [https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition\\_en](https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en).

- National Cyber Crime Contact Point pursuant to Article 35 of the Convention on Cybercrime (the Budapest Convention, ETS No. 185)
- Contact Point pursuant to Article 13 – Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013, on attacks against information systems – in cooperation with the national investigation division
- Contact Point pursuant to the EU Law Enforcement Emergency Response Protocol to handle major cross-border cybersecurity attacks – in cooperation with the national investigation division
- Contact Point for the Czech Banking Association (CBA), for an administrator of .cz domain and a national CSIRT team (CZ.NIC)
- Contact Point – G7 24/7 HTC Network.

The main tasks pursuant to Article 35 of the Convention on Cybercrime are:

- provision of technical advice
- preservation of data
- collection of evidence
- provision of legal information
- localization of suspects and missing persons
- communication with the other contact points on an expedited basis.

The four-year development of the fight against cybercrime based on the presented Concept was successful. This was confirmed in the Resolution of the National Security Council of the Czech Republic on June 8, 2020, approving the “Final Report on the Fulfillment of Tasks Resulting from the Concept for the Development of the Cybercrime Investigation Capabilities of the Police of the Czech Republic.” It also decided on the development of a new strategy to combat cybercrime.

The fact that the issue of cybercrime is still evolving dynamically and the ever-more-notable increase in crime in the virtual world suggests that even greater efforts will be needed in the future to tackle cybercrime. Towards this end, attention will be required from law enforcement agencies and other security experts, whether in the civil service or the private sector. Cyberspace has become an integral part of our daily lives, which poses a number of risks and needs to be properly secured.

In the 21<sup>st</sup> century, it will be necessary to focus not only on the common crime committed in the virtual world but also on securing critical information infrastructure. This is a comprehensive problem that affects all levels of the security system and includes crisis management. It is necessary to realize that critical infrastructure is essential for society and the functioning of a democratic state and a cornerstone of a thriving economy. Its protection is therefore vital in order to prevent the escalation of incidents into crises.

The security of critical information infrastructure in cyberspace can be divided into three basic levels: cyber defense, cyber security, and cybercrime. Institutionally speaking, the provision of security requires effective and coordinated activities of the armed forces, the relevant cyber security office (The National Cyber and Information Security Agency; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), the security forces (especially the Police of the Czech Republic), eventually the intelligence services, as well as the private sector.

The state's role also lies in setting basic security standards and legally enforcing them on the private sector. However, these measures must not be financially detrimental, and the state must ensure the adequate protection of cyberspace. It should be borne in mind that a significant part of the state's critical infrastructure is not in its exclusive ownership. The state merely participates in its management in a majority or minority role.

Related to this is the further need to define the division of cybercrime in order to give space to computer technology experts to detect, document, and investigate serious cases of cybercrime, such as attacks on cyber information infrastructure and essential information systems, which may have different origins, including the most serious ones such as terrorism or espionage.

To this end, cybercrime has been redefined, namely as:

- a crime committed in the environment of information and communication technologies, including computer networks where the main target of the attack is the area of information and communication technologies itself and the data contained in them; it follows that the primary attention of experts will be on meeting the established criteria – examples are § 230 Unauthorized Access to a Computer System on an Information Carrier, and § 231 Acquisition and Encoding of an Access Device and Password to a Computer System and Other Similar Data;
- any other crime committed in cyberspace, defined as a crime committed with the significant use of information and communication technologies where the main target of the attack is primarily life, health, property, freedom, human dignity, and morality.

## Conclusion

For the reasons mentioned above, a new cybercrime strategy will need to be developed in the near future, which will need to consider many factors, including close cooperation among the various partners who play an important role in ensuring the security of cyberspace. The new strategy is to be submitted to the Security Council of the Czech Republic in 2021. It cannot be ruled out that it will be influenced by the COVID-19 pandemic, which forced a large part of society to work and spend its free time on the Internet; for some, it became a second living space. Last but not least, it can also focus on cyber defense against ransomware attacks on critical information infrastructure by criminal organized groups as well

as hostile powers and their investigation. Another serious future challenge will be the fight against disinformation campaigns, which, however, will require more comprehensive cooperation across the entire security system, and not only in the Czech Republic.

The Budapest Convention on Cybercrime can be used as a good example of how to approach other security challenges in cyberspace. Therefore, I can state with peace of mind that the Czech Republic is on the right track in the fight against cybercrime and believe that it will make the needed enhancements in the future.

## Disclaimer

The views expressed are solely those of the author and do not represent official views of the PFP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## Acknowledgment

This article presents research results from the project V20192022117 "Detection of Radicalization in the Context of Protection of the Population and Soft Targets from Violent Incidents," supported by the Ministry of the Interior of the Czech Republic.

## About the Author

**Lukáš Vilím** is Lieutenant Colonel in the National Organized Crime Agency in the Ministry of the Interior of the Czech Republic, a police officer in the Cybercrime Unit of the Criminal Police and Investigation Service in Prague. He holds a Ph.D. degree from the Police Academy in Prague. Dr. Vilím is a graduate of the Cyber Security Studies program and the European Security Seminar-East of the George C. Marshal Center.

E-mail: lukas.vilim@email.cz



## Trusting ICT Providers – Can Corporate Cyber Confidence-Building Measures Help?

**Matthias Klaus**

**Abstract:** Trust in cyberspace is essential for increasing security and even more important when nations rely on private companies to develop, construct, maintain and operate their Information and Communication Technology infrastructures. This article proposes a redesigned form of Cyber Confidence-Building Measures to achieve this goal by including the private sector as a peer actor. Nations can use this method to vet their potential suppliers, so they may reduce their risk perception and establish and maintain a trustful relationship with them.

**Keywords:** trust, supply chain security, cyber risk, ICT infrastructure, cyber confidence-building measures.

### Introduction

Nations need to trust or ban a vendor from building their Information and Communication Technology (ICT) infrastructure and services. In a world where private companies almost exclusively wield both the technical expertise and means to develop, operate, and maintain the ICT structure, nations increasingly depend on the private sector. As it is impossible to determine the integrity of supplied software or hardware, trust between customer and supplier is paramount, mirroring the classic trust issues between citizens, government, and corporations.<sup>1</sup> A nation will choose a company it trusts to protect its interests against security-related risks. It will continue to assess the ICT providers on their trustworthiness and transparency. In a situation where a nation may not have trusted options available, it must settle on a company nonetheless. The Prague Proposals of 2019, the results of an international conference on 5G security, acknowledge this as one of the most important policy-related security

---

<sup>1</sup> George Cvetkovich and Ragnar E. Löfstedt, eds., *Social Trust and the Management of Risk* (London: Earthscan, 1999).

risks in managing a nation's IT infrastructure.<sup>2</sup> This task is critical and increasingly complex, especially when one of the most prominent candidates, Huawei, is under suspicion of being controlled by the Chinese Communist Party (CCP).

The focus of this article is to propose a way to build trust by drawing upon the lessons learned from the Huawei challenge. Specifically, this article presents a way forward for distrusted nations and companies alike by proposing an adjusted form of Confidence-Building Measures (CBMs) to promote trust and reduce the risk perception of their potential customers. For customer nations, it could offer assurance in selecting a suitable ICT provider, while for suppliers, it provides the possibility to prove their transparency and independence from other actors. In a post-trust world, this kind of transparent and proactive communication could help rebuild trust and prevent a breakdown of communication between actors from rivaling political systems.<sup>3</sup>

## The Case of Huawei

Huawei is a leading ICT company that has grown through substantial state subsidies and preferential treatment for China's domestic market.<sup>4</sup> Huawei's status as a "national champion" of a high-profile industry such as ICT<sup>5</sup> enabled it to become the world's largest telecom equipment and second-largest smartphone manufacturer.<sup>6</sup>

Huawei claims to be a private company,<sup>7</sup> yet its internal organization differs from the classic understanding of one. Huawei's prime argument is that the company's employees are also its owners, with nearly 87,000 shareholders voting for the Representative Commission. This Commission elects the Board of Directors and Supervisory Board, which then elect the Executive Committees.<sup>8</sup>

<sup>2</sup> "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World," Prague 5G Security Conference, Prague, May 3, 2019, accessed March 12, 2020, [https://www.vlada.cz/assets/media-centrum/aktualne/PRG\\_proposals\\_SP\\_1.pdf](https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf).

<sup>3</sup> Ragnar E. Löfstedt, *Risk Management in Post-Trust Societies*, Earthscan Risk in Society series (London: Earthscan, 2008).

<sup>4</sup> "The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks," *Strand Consult*, 2019, p. 12, accessed February 1, 2020, <https://strandconsult.dk/the-real-cost-to-rip-and-replace-chinese-equipment-from-telecom-networks>.

<sup>5</sup> Tai Ming Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities," *Journal of Cyber Policy* 3, no. 3 (2018): 306-326, 311, <https://doi.org/10.1080/23738871.2018.1556720>.

<sup>6</sup> Elsa Kania, "Much Ado about Huawei (part 1)," *The Strategist* (Australian Strategic Policy Institute), March 27, 2018, accessed March 9, 2020, <https://www.aspistrategist.org.au/much-ado-huawei-part-1>.

<sup>7</sup> "Huawei's Position Paper on Cyber Security" (Huawei, November 2019), 61, accessed March 12, 2020, [www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en](http://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en).

<sup>8</sup> "Who Runs Huawei: Ownership and Governance," *Huawei*, accessed March 24, 2020, <https://www.huawei.com/minisite/who-runs-huawei/en>.



While true to a degree, the company's representation leaves out crucial details regarding its ties to the CCP, the most important being that 99% of the shares are not owned by its founder or the employees but by the Huawei Investment & Holding Trade Union Committee (TUC). Furthermore, the Huawei Investment & Holding TUC is ultimately answerable to the All-China Federation of Trade Unions, whose head sits on the Central Political Bureau of the Chinese Communist Party (CCP).<sup>9</sup> Another factor to consider is the involvement of the CCP in the company, as evidenced by the current Chief Ethics & Compliance Officer being a party secretary.

Chinese state-owned banks also treat Huawei similarly to state-owned companies. For example, the China Development Bank, which is under the control of the Chinese government and the biggest holder of loans worldwide, is the main funder of Huawei.<sup>10</sup> A risk profile from 2018 shows that Huawei also received billions of dollars in funding from several state banks in China.<sup>11</sup> The 2018 arrest of Huawei's Chief Financial Officer, who was in possession of eight different passports, including a "public affairs" passport usually reserved for state-related officials, casts further doubt on the asseverations of independence.<sup>12</sup>

Adding to the distrust is China's use of cyber espionage. Critics claim that China is incapable of differentiating between the political-military espionage conducted by every nation and large-scale, economically motivated theft of intellectual property against economic rivals. To make matters worse, the CCP shares the results of its ill-gotten gains with Chinese companies to further provide them with economic advantages besides its generous state subsidies.<sup>13</sup> State support is arguably what made Huawei successful, as it allowed Huawei to expand rapidly and undercut competitors.

Another concern involves China's ability to compel companies to cooperate with its intelligence services. The 2017 Intelligence Law contains articles interpreted as a way for Chinese intelligence services to either access Huawei ICT it-

---

<sup>9</sup> Christopher Balding and Donald C. Clarke, "Who Owns Huawei?" *SSRN Journal*, April 17, 2019, <https://doi.org/10.2139/ssrn.3372669>.

<sup>10</sup> Bob Seely, Peter Varnish, and John Hemmings, "Defending Our Data: Huawei, 5G and the Five Eyes," *Henry Jackson Society*, Asia Studies Centre, May 16, 2019, p. 26, accessed February 1, 2020, <https://henryjacksonsociety.org/publications/defending-ourdata>.

<sup>11</sup> RWR Advisory Group, "A Transactional Risk Profile of Huawei," February 13, 2018, p. 20, accessed March 17, 2020, <https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf>.

<sup>12</sup> Michael Mui, "How Meng Wanzhou's 'P' Passport Works," *The Star*, January 23, 2019, <https://www.thestar.com/vancouver/2019/01/23/how-meng-wanzhou-s-p-passport-works.html>.

<sup>13</sup> Su-Mei Ooi and Gwen D'Arcangelis, "Framing China: Discourses of Othering in US News and Political Rhetoric," *Global Media and China* 2, no. 3-4 (2017): 269-283, 275, <https://doi.org/10.1177/2059436418756096>.

self or force the company to cooperate.<sup>14</sup> In particular, Article 7 gives cause for scrutiny. China has assured that Article 7 is misunderstood and poses no security risk.<sup>15</sup> In response, Huawei tasked a Chinese law firm to confirm this,<sup>16</sup> but critics have pointed out that legal assessments do not adequately address the concerns.<sup>17</sup> At the moment, it is reasonable to assume Huawei's non-compliance with Article 7 would hurt its standing with the CCP.

In an effort to strengthen confidence in the company, in 2019, Huawei's chair offered to sign a "no spy agreement" with the United Kingdom, Germany, and India.<sup>18</sup> However, this offer failed to gain other countries' confidence because Huawei does not behave like a private corporation. For example, Huawei states that it does not intend to go public due to moral reasons. Seely, Varnish, and Hemmings<sup>19</sup> suspect that the real reason may include "legal requirements to report company structure, auditing data, and financial statements relating to cash flow, equity, and balance sheets to the public, to public shareholders, and to authorities such as the US Securities and Exchange Commission." Additionally, Seely and colleagues<sup>20</sup> note that the "absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection" are signs of risk concerning Chinese technology firms under the given context.

A growing number of nations have banned Huawei equipment in their networks, citing risk concerns with Huawei's close ties to the CCP and fears of surveillance. Currently, the United States, the United Kingdom, Japan, Taiwan, Australia, New Zealand, Sweden, the Czech Republic, Denmark, Estonia, Guernsey, Jersey, Latvia, Poland, and Romania are among the countries banning Huawei. Developing countries seem to be less wary of the security risks. In most cases, this is related to the simultaneous granting of loans and other forms of assistance offered by Chinese state-owned organizations,<sup>21</sup> helping developing countries to overcome the barriers to technology acquisition.

---

<sup>14</sup> People's Republic of China, National Intelligence Law of the People's Republic, June 27, 2017.

<sup>15</sup> Bonnie Girard, "The Real Danger of China's National Intelligence Law," *The Diplomat*, February 23, 2019, accessed May 2, 2020, <https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law>.

<sup>16</sup> Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

<sup>17</sup> Samantha Hoffman and Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist* (Australian Strategic Policy Institute, September 13, 2018, accessed March 17, 2020, [www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws](http://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws)).

<sup>18</sup> "Huawei Answers on Cybersecurity," *Huawei*, October 21, 2019, accessed February 26, 2020, <https://www.huawei.eu/story/huawei-answers-cybersecurity>.

<sup>19</sup> Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

<sup>20</sup> Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

<sup>21</sup> Cheung, "The Rise of China as a Cybersecurity Industrial Power," 323.

## The Gap: Cyber Confidence-Building Measures

In the absence of universally binding regulations, nations use CBMs, originating from regular arms control norms, to build trust between each other in cyberspace. To date, there are no internationally universally recognized and binding norms of acceptable behavior in this realm. The international community agreed that existing international laws, such as the Charter of the United Nations (UN), apply in cyberspace.<sup>22</sup> However, there is division over the question of how to apply and enforce these laws to specific cyber operations. This is in part because existing laws were not designed with cyber activities in mind. Another reason is the lack of consensus among nations on the terms and definitions necessary to formulate acceptable binding regulations. This is often because of a lack of trust or goodwill to compromise with opposing nations due to the high-risk perception towards trusting actors holding different values than oneself.<sup>23</sup>

CBMs are intended to reduce risks or the perception of risks by building trust and improving the relationship between the participating nations. Cyber CBMs (CCBMs) aim to establish stable international relations and a common understanding of acceptable state behavior in cyberspace.<sup>24</sup> They encompass information exchanges and cooperation between nations to combat illegal cyberattacks of various forms.<sup>25</sup> Due to their origin in classical arms control, international actors can also constitute CCBMs as bilateral or multilateral agreements.<sup>26</sup> They increase the overall feeling of security among nations by demonstrating the good intention of all participants.<sup>27</sup> CCBMs can also facilitate an exchange of respective working methods and practices, as well as mutual expectations concerning behavior. Since norms reflect the standard behavior ex-

---

<sup>22</sup> UN General Assembly, “Developments in the Field of information and Telecommunication in the Context of International Security,” Resolution 70/237 Adopted by the General Assembly on December 23, 2015, accessed March 18, 2020 (United Nations, 2015), <https://undocs.org/en/A/RES/70/237>.

<sup>23</sup> Michael Siegrist, George Cvetkovich, and Claudia Roth, “Salient Value Similarity, Social Trust, and Risk/Benefit Perception,” *Risk Analysis: An International Journal* 20, no. 3 (2000): 353-362, <https://doi.org/10.1111/0272-4332.203034>.

<sup>24</sup> Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013).

<sup>25</sup> Geun Hye Kim, Kyung Bok Lee, and Jong In Lim, “CBMs for Cyberspace beyond the Traditional Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia,” *The Korean Journal of Defense Analysis* 27, no. 1 (2015): 87-106.

<sup>26</sup> Arnold Kraesten, “Cyber Confidence-Building Measures. Ten Stumbling Blocks Which Complicate the Development and Implementation of Worldwide Politically Acceptable Cyber Confidence-building Measures,” MSc in Cyber Security, with assistance of Sergej Boeke (The Hague, 2016).

<sup>27</sup> Erica D. Borghard and Shawn W. Loneragan, “Confidence Building Measures for the Cyber Domain,” *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), accessed December 26, 2019, <https://www.hsdl.org/?view&did=815333>.

pected by nations in cyberspace, CCBMs and norms often complement each other.<sup>28</sup>

CCBMs are designed for interactions between state actors; therefore, they are not currently applied to state-to-non-state actor interactions. Most experts agree that CCBMs must also take the multi-stakeholder nature of the cyber domain into account, which includes private corporations, amongst others.<sup>29</sup> However, traditional international and regional organizations, such as the UN and the Organization for Security and Co-operation in Europe (OSCE), which primarily focus on state relations, are the entities mainly developing CCBMs and cyber norms.<sup>30</sup> While this makes sense for CBMs, where states are the sole wielders of military and nuclear power, it falls flat in cyberspace. Here, the power, by design, does not rest with the states alone but also with technology companies, which develop and operate most of the critical infrastructure, such as 5G networks.

### Proposal: Evolution of CCBMs to Include Non-state Actors

An article by Hitchens and Gallagher compared the progress achieved by both the UN Group of Governmental Experts (GGE) and OSCE on norm-building and CCBMs in April 2019. It made two points of value for this article. First, the authors emphasized the importance of the relationship between a nation-state and non-state actors, focusing on information sharing and risk assessment.<sup>31</sup> Second, they recommended an increase in participation of stakeholders to include “companies that own or operate key parts of the ICT infrastructure ... along with some private-sector cybersecurity service providers,”<sup>32</sup> paralleling recent statements by the OSCE and UN GGE. Both nation-states and non-state actors, such as private companies, need to take part in developing and applying CCBMs.

The reasons given for the current lack of ICT industry involvement in CCBM development are “lack of government understanding of the cyber-sphere, heavy-handed regulation and the efforts of national security organizations to

<sup>28</sup> Patryk Pawlak, “Confidence-Building Measures in Cyberspace: Current Debates and Trends,” in *International Cyber Norms: Legal, Policy & Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE Publication, (2016), 129-153, [https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms\\_Ch7.pdf](https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch7.pdf).

<sup>29</sup> Jason Healey, John C. Mallery, Klara J. Tothova, and Nathaniel V. Youd, “Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security,” Report (Atlantic Council, November 5, 2014), accessed December 30, 2019, <https://atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security>.

<sup>30</sup> Borghard and Lonergan, “Confidence Building Measures for the Cyber Domain.”

<sup>31</sup> Theresa Hitchens and Nancy W. Gallagher, “Building Confidence in the Cybersphere: A Path to Multilateral Progress,” *Journal of Cyber Policy* 4, no. 1 (2019): 4-21, <https://doi.org/10.1080/23738871.2019.1599032>.

<sup>32</sup> Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

compromise private sector tools and networks for their own uses.”<sup>33</sup> Hitchens and Gallagher, in the tradition of classic CCBMs, call for better cooperation to improve the integration of private companies. However, this article proposes a different interpretation of the circumstances described in this quote. It is exactly the lack of government understanding of the cyber-sphere that puts companies in an advantageous position to compromise a state’s attempts to regulate cyberspace. Therefore, nations should be interested in making ICT providers more than just stakeholders in the CCBM process; they should endeavor to make them subjects on equal footing.

The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) differentiates between two sets of CCBMs. One is a demand-driven model, where norms for acceptable behavior in cyberspace trigger the development of concurrent CCBMs, which result in increasing cyber capacities. The other is a supply-driven model, which sets advancing cyber capacities, often developed and implemented by non-state actors, as the trigger to develop “concrete cooperative CBMs between all stakeholders.”<sup>34</sup> These CCBMs result in new norms being formulated to guide nations on how to use the new capabilities.

Pawlak intended to use non-state actors to improve inter-state relations, but the distinction between the different models of CCBMs is valuable for this article. This article argues that with the development of groundbreaking technologies in cyberspace, such as 5G, there is a need to develop CCBMs to reduce the risks perceived by stakeholders. As seen in the current debate about Huawei’s inclusion or exclusion in the 5G networks of several countries, these groundbreaking technologies, yet to be fully developed or even understood, are ripe for exploitation.

As described in the 2019 Prague Proposals, a risk assessment needs to cover both potential technical and non-technical threats posed by a supplier. Issues such as the legal environment of its origin nation, the form of governance, and security cooperation all need to be accounted for.<sup>35</sup> The Charter of Trust (CoT)—a consortium of technology companies calling for binding rules and standards—offers an interesting approach to creating trust amongst ICT suppliers. It focuses on supply chain management and has a very important statement for the case in this article: “The CoT partners also believe that no undocumented functionalities or possibilities for remote connection should be part of initial device setup; another aspect that is not yet a general rule today.”<sup>36</sup> It acknowledges that not only companies but also governments could come into a

---

<sup>33</sup> Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

<sup>34</sup> Pawlak, “Confidence-Building Measures in Cyberspace.”

<sup>35</sup> “The Prague Proposals: The Chairman Statement on Cyber Security.”

<sup>36</sup> “Charter of Trust Partners Decide on Further Measures for More Cybersecurity,” *Charter of Trust*, February 14, 2020, accessed March 27, 2020, <https://www.charteroftrust.com/news/charter-of-trust-partners-decide-on-further-measures-for-more-cybersecurity>.

situation where the inherent risks of ICT require the establishment of rules concerning identity and access management.<sup>37</sup>

There is an emerging trend to include actors beyond nations in regulating the cyberspace, but the inclusion of non-state actors so far is limited to advisory or feedback roles. The idea to make the private sector a counterpart to a nation under the conditions of a CCBM represents a new approach, which was only recently alluded to in a report by the Global Commission on the Stability of Cyberspace (GCSC) in the form of norms for cyberspace for both states and non-state actors.<sup>38</sup>

As outlined in the previous section, a deep lack of trust hinders potential business between Huawei and several nations. Huawei's Position Paper on Cyber Security shows the company is acutely aware of this, as it dedicates an entire chapter to addressing its "business independence." The company even declared its willingness to sign a "no spy" agreement and would rather shut down the company than infringe on customer privacy and security.<sup>39</sup> However, this declaration will do little to convince critics as it is a publicity statement and does not actively build trust, which is exceedingly difficult once lost.<sup>40</sup> The supply-driven model mentioned earlier comes into play here. As the new technologies offered by Huawei are perceived as risky, stakeholders like interested nations should develop CCBMs to deal with them.

Next, this article will examine the Huawei Cyber Security Evaluation Center (HCSEC), which tests Huawei's equipment and discerns risks in software or hardware, as a potential basic model for more advanced measures. The HCSEC was established in 2010 and staffed by Huawei, with the UK's National Cyber Security Centre (NCSC) acting as a direct counterpart to the company. The HCSEC oversight board is chaired by the CEO of the NCSC and includes a Huawei senior executive, several UK government officials, and experts from the private sector. Since 2014, the oversight board has produced annual reports, including an audit to show its ability to operate independently of Huawei Headquarters.<sup>41</sup> The HCSEC aims to "demonstrate an increase in Huawei's

<sup>37</sup> "Our 10 Principles: Cybersecurity Concerns Us All," *Charter of Trust*, accessed March 27, 2020, <https://www.charteroftrust.com/about>.

<sup>38</sup> Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, Final Report (Global Commission on the Stability of Cyberspace, November 2019), accessed January 1, 2020, <https://cyberstability.org/report/>.

<sup>39</sup> "Huawei's Position Paper on Cyber Security."

<sup>40</sup> Paul Slovic, "Perceived Risk, Trust, and Democracy," *Risk Analysis: An International Journal* 13, no. 6 (1993): 675-682, <https://doi.org/10.1111/j.1539-6924.1993.tb01329.x>.

<sup>41</sup> Huawei Cyber Security Evaluation Centre Oversight Board, "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020: A Report to the National Security Advisor of the United Kingdom," Part I: Summary, September 2020, accessed November 2, 2020, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/923309/Huawei\\_Cyber\\_Security\\_Evaluation\\_Centre\\_HCSEC\\_Oversight\\_Board-annual\\_report\\_2020.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre_HCSEC_Oversight_Board-annual_report_2020.pdf).

technical capability” and software engineering. However, it also aims to “continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns,”<sup>42</sup> which aligns with the concept of a CCBM. But the review of technical capabilities alone does not address the root of the problem.

In the case of Huawei, the center rather needs to deal with the issues of actual ownership, independence from the influence of the CCP, and the Intelligence Law of 2017. These questions trace back to Huawei’s country of origin, which again corresponds to the risk assessments outlined in the Prague Proposals. While the HCSEC reported having found no evidence of the Chinese state’s involvement with the discovered technical deficiencies, this did not convince critics. If one believes Huawei collaborates with the CCP and Chinese intelligence services, an apparent lack of installed technical backdoors will be insufficient proof. Given the rapidly developing technology, the code could later be tampered with via updates. An undisclosed relationship between Huawei and Chinese intelligence services is a major roadblock to building trust.

## **Policy Recommendations**

This article acknowledges that Huawei would most likely not agree to the CCBMs, despite their claims towards transparency. However, this is not the point this article tries to make. Instead, it proposes to adjust and apply the supply-driven model as a general measure embedded in a country’s selection process for ICT providers. CCBMs hold the promise to build trust between nations and ICT companies and contribute to security in cyberspace by establishing norms of transparency.

*Recommendation #1:* First, nations should build their own independent Corporate CCBM (C3BM) agencies, staffed and led by government experts in the ICT field. These institutions would have the mission to vet potential suppliers of national key ICTs and assess the risk associated with them. They should subsequently develop adequate C3BMs to counter the risks identified in each company. If interested in doing business with a nation, an ICT company must then abide by the measures to build up the trust to be accepted as a supplier. An added benefit of using a C3BM is that the review results could be shared with other nations, thus reducing the redundancy for ICT companies. Countries that are unable to create their own agency can use the C3BM reports of other nations as a baseline for their ICT contracts. Alternatively, several nations could pool their resources and create a C3BM agency at a regional level. Here, they should synchronize their expected transparency standards and develop unified conditions for business with private companies.

---

<sup>42</sup> Huawei Cyber Security Evaluation Centre Oversight Board, “Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020,” Part II: Section I.



In the case of Huawei, a C3BM agency could identify the risks discussed earlier and develop matching measures to address them. One approach could be the condition for Huawei to implement transparency measures equal to its European competitors Ericsson and Nokia. As illustrated by a recent Strand Report, these competitors outclass Huawei in both financial and technological transparency.<sup>43</sup> This includes transparency for third-party code use, which is an additional security issue of Huawei's underlying software platform, as it is notoriously hard to verify.<sup>44</sup> Another C3BM could be the concept of establishing a national branch of Huawei as a completely separate entity with shared ownership between Huawei and a domestic private or state-owned company, with the servers based inside the nation.

*Recommendation #2:* Nations should propose this new and expanded definition of CCBMs to international and regional organizations so that non-state actors are recognized as active partners for nations and subjects to CCBMs. An international organization, such as the UN, could be reluctant to accept the idea of non-state actors becoming equal counterparts to nation-states. However, regional organizations, such as OSCE and the Organization of American States, should be more accepting of non-state actors since many confidence-building mechanisms are established at the regional level.

If such organizations begin accepting this expanded definition of CCBMs, it will lend legitimacy to the concept. This would motivate private companies to adapt to C3BMs and prepare accordingly before approaching nations to conduct business with them. As nations move toward the 4th Industrial revolution, there will be an ever-expanding dependence on the private sector for developments in AI, surveillance, biotechnology, and quantum computing. These emerging technologies will pose other future challenges and risks yet to be defined or conceptualized. Since many of these technologies are dual-use, meaning they have military and civilian applications, there is an even greater need to start building trust between nations and the private companies developing the technologies.

---

<sup>43</sup> "The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks."

<sup>44</sup> Jiwon Seo and Monica S. Lam, "InvisiType: Object-Oriented Security Policies" (Stanford University, Computer Systems Laboratory, 2010), p. 1, accessed December 7, 2020, <https://suif.stanford.edu/papers/ndss10.pdf>.



## **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **About the Author**

**Matthias Klaus** is an international security and risk analyst. With experience as a squad and platoon leader and instructor in the German Armed Forces, Matthias joined the Master of Arts in International Security Studies (MISS) program, delivered jointly by the George C. Marshall Center and the Universität der Bundeswehr München.

E-mail: [mk2124@cam.ac.uk](mailto:mk2124@cam.ac.uk)





## Cyber Skills Gaps – A Systematic Review of the Academic Literature

**Harri Ruoslahti,<sup>1</sup> Janel Coburn,<sup>1</sup> Amir Trent,<sup>1</sup>  
and Ilkka Tikanmäki<sup>1,2</sup>**

<sup>1</sup> *Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland, <http://www.laurea.fi/en>*

<sup>2</sup> *Department of Warfare, National Defence University, Helsinki, Finland, <https://maanpuolustuskorkeakoulu.fi/en>*

**Abstract:** This literature review is part of research on the roles of and training for e-skills in modern society, specifically, the role of cyber skills. This article explores how the academic literature discusses cyber skills and identifies e-skills that can be determined as necessary for the functioning of society today. First, the introduction provides an explanation of the overall impact of cyber skills in our modern-day society. Next, the body presents the method used to conduct the review and a concise summary of the findings to answer our research questions. Finally, based on the research findings, the conclusions address the feasibility, impact, strengths, weaknesses, and possible ethical concerns.

**Keywords:** society, cybersecurity, cyber training, e-learning, cyber skills.

### Introduction

The use of computers and other digital technology is a daily reality for over half of the global population and substantially more in modern European society. Of the roughly 7.8 billion people inhabiting the planet as of March 2020,<sup>1</sup> an

---

<sup>1</sup> Joseph Chamie, "World Population 2020: Overview," *Yale Global Online*, February 11, 2020, accessed April 12, 2020, <https://yaleglobal.yale.edu/content/world-population-2020-overview>.

estimated 59% are internet users and, as of 2019, 49% of those users have computers in their homes.<sup>2</sup>

Looking at the numbers above, it is logical to assume that a set of e-skills have become a prerequisite to functioning in society today. Therefore, the purpose of this literature review was to understand how cyber skills relate to e-skills and specifically to identify gaps and cyber skills that meet these gaps as they are discussed in the academic literature.

Project ECHO<sup>3</sup> (European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations), which started in 2019, aims at strengthening proactive cybersecurity in the European Union via a networked approach of effective and efficient multi-sector collaboration. This study adds to the body of knowledge, which the project cumulates, identifying how training for cyber skills is discussed in the academic literature and how they may relate to the broader spectrum of e-skills and the respective training can help design practical measures to identify and train focused cyber skills as part of a more general range of e-skills. In planning this study, we examined e-skills as skills needed to function in today's digital world, i.e., physically operate computers and smart devices and efficiently use the programs, applications, and digital information.

The cyber skills framework developed within the ECHO project represents an approach to describe the cyber skills requirements used to create the training curricula to equip cybersecurity professionals with the needed expertise to address the identified sectoral, transversal, and multi-sector cybersecurity challenges.<sup>4</sup> In addition, defining specific cybersecurity skills and related curricula for all levels of staff could fix the lack of awareness limiting responsivity to attacks. As described in ECHO research, cyber curricula and skills would help the healthcare and other sectors make a considerable step towards an entirely new level of cybersecurity.<sup>5</sup>

According to Chamie,<sup>6</sup> modern society has evolved into a technology-driven world due to the emergence of the Internet. The Internet has modified every aspect of social dynamics, from how business is being conducted (transforming traditional companies into digital-oriented firms) to how learning is being facilitated (e.g., with e-learning platforms) and how people interact with each other

<sup>2</sup> Statista, "Share of Households with a Computer at Home Worldwide from 2005 to 2019," March 2, 2020, accessed April 11, 2020, <https://www.statista.com/statistics/748551/worldwide-households-with-computer>.

<sup>3</sup> European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Grant Agreement Number: 830943 – ECHO – H2020-SU-ICT-2018-2020/H2020-SU-ICT-2018-2 (2019).

<sup>4</sup> European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 121.

<sup>5</sup> European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 64.

<sup>6</sup> Chamie, "World Population 2020."

(thorough social networking platforms). With the advances in information and communications technology (ICT) tools, such as handheld mobile devices that provide constant and instant access to the Internet, people are more connected to ICT than ever before. ICT is essentially an integral component of our everyday lives. Besides the many benefits of utilizing the Internet and other ICT technology, there are unfortunately also threats, e.g., by cyber attackers who, with malicious intent, look to exploit vulnerabilities within these ICT applications. In order to delve into the significance behind developing cyber skills, this literature review focuses on cyber training and cyber skills development in relevant articles. The purpose of this review is to extend upon current knowledge regarding ICT training. To put this into perspective, the research questions of this study are:

RQ1: How does the academic literature discuss cyber skills gaps?

RQ2: What measures does the academic literature suggest in filling these gaps?

## **Methods**

The main method used in this research is a systematic literature review. This is a qualitative study, and the main reason behind performing this systematic modern literature review is to identify the knowledge gaps of modern society pertaining to cyber skills to bring new insights to the field of e-skills development for further investigation.<sup>7</sup>

### ***Qualitative Research Design***

According to Kitchenham,<sup>8</sup> the systematic literature review is a thorough process that can help present evidence displaying the effects of certain events described in research and could not be conveyed in traditional non-systematic literature reviews. Systematic literature reviews may also be more extensive than regular ones. To perform this literature review, an academic search was conducted to find answers to the research questions. This study was conducted in a series of four steps: search, selection criteria, DET (data extraction table) analysis, and writing of the findings and conclusions.

### ***Search***

The search for articles was performed in March 2020. The search was conducted using the scientific databases ProQuest Central and EBSCO Host. The combination of “cyber security training” and “e-skills training” was used as search parameters in a Boolean keyword search. The period for the search spanned literature published within the ten years of 2010-2020.

---

<sup>7</sup> Barbara Kitchenham, “Procedures for Performing Systematic Reviews,” Joint Technical Report TR/SE-0401 (Keele, UK: Keele University, 2004): 1-26, <https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf>.

<sup>8</sup> Kitchenham, “Procedures for Performing Systematic Reviews.”

The ProQuest Central database search returned a total of 67 peer-reviewed articles, and the EBSCO Host database search returned two additional peer-reviewed articles. A final sample was selected for further analysis by applying inclusion criteria to the 67 articles in the initial keyword search. The inclusion criteria applied to the original 69 papers are: title or abstract includes themes related to cyber or e-skills training in the workforce and cyber or e-skills training in higher education. Applying the inclusion criteria rendered a final sample of 21 peer-reviewed articles (Table 1), which were all read thoroughly for analysis.

**Table 1. Steps of Search and Resulting Numbers of Academic Papers.**

Search Steps	Papers in Sample
Initial search results from ProQuest Central and EBSCO Host	69
After applying the Inclusion Criteria	21

The analysis of the final sample was done by extracting relevant pieces of information to a data extraction table (DET) based on the research questions. The next section discusses the findings from the sample of 21 articles.

## Findings

### *Focus on Cyber Skills*

The results indicate that cybersecurity is a significant concern in modern society. As new technologies with network capacity are being developed in connection with critical infrastructures and everyday activity, cyber devices are becoming vulnerable to cyberattacks by malicious actors. Spanning from identity theft to cyberbullying, these attacks can significantly influence financial, economic, and social systems. The large percentage of articles that did not meet the inclusion criteria indicates that many authors have a rather technological or risk-related focus on cybersecurity.

The articles included in the final sample indicate that most people who have access to ICT devices are at risk. People are either not sufficiently knowledgeable in cybersecurity or fail to practice proper cybersecurity measures. Challenges regarding cybersecurity vary depending on the age of the audience. Younger generations are more susceptible to cyber-attacks for several reasons: not practicing security measures, over-reliance on the security on their personal devices, lack of familiarity with new technologies centered around social media, or being most active in online shopping. Oversharing personal information in social networking sites or sites that third parties can harvest also contributes to the increased cybersecurity risk.

Overall, it is noteworthy that e-skills had significantly fewer mentions than cyber-related skills. Cybersecurity-related skills in the workplace and professional work are at the forefront of the discussions. Seventeen out of 21 peer-

reviewed articles addressed cybersecurity skills, cybersecurity training, or information/network security-related items. In fact, the search term “e-skills” produced only one result, and the other three remaining articles were found based on the keyword “e-learning.” Based on these facts, one initial finding of the literature review is that the academic publications much more often discuss current cybersecurity threats, lack of cyber-related training and qualifications to deal with modern cyber threats, and new ways to provide training addressing cybersecurity threats.

The analysis of the data from the 21 sourced articles regarding e- and cyber skills found four major thematic categories.

1. General Cybersecurity: eight articles discuss the need and applications of cybersecurity training, awareness, and literacy.
2. Cybersecurity Training and Education: seven articles discuss the need for cyber education among certain academic programs, recommend cybersecurity training and education methods, and look at the differences between cyber education and cyber training. Cyber Ranges and Exercises emerged as a sub-category of Cybersecurity Training and Education. These articles discuss what these ranges and exercises are as training mechanisms and how they operate.
3. E-learning: five articles define e-learning, present barriers to e-learning, the need for ICT skills before e-learning can be accomplished, and discuss effective and specific, hands-on practical approaches for e-learning to be successful.
4. E-skills: only one primary article discusses an EU-wide need to increase ICT skills, why these e-skills are needed in everyday work and personal life, and how it affects the EU and global economy.

Eight out of the twenty-one articles make specific mentions of skills needed to operate professionally or in a personal capacity in everyday life or cybersecurity-related skills required to prevent malicious internet actors from achieving success. The one article that discusses specifically e-skills creates categories according to the level of e-skills needed to operate in daily work life. According to Singh,<sup>9</sup> these function categories are ICT practitioner skills, ICT user skills, and e-business skills.

### **General Cybersecurity**

Table 2 below gives an overview of the eight papers that focus on cybersecurity training in general and their respective foci.

---

<sup>9</sup> Sumanjeet Singh, “Developing e-Skills for Competitiveness, Growth and Employment in the 21<sup>st</sup> Century: The European Perspective,” *International Journal of Development Issues* (Emerald Group Publishing) 11, no. 1 (2012): 37-59, <https://ideas.repec.org/a/eme/ijdipp/v11y2012i1p37-59.html>.

**Table 2. Articles that Relate to General Cybersecurity.**

Article	Topic
Ricci et al. (2019) <sup>10</sup>	Survey results on adults and cybersecurity education
Clifton (2018) <sup>11</sup>	Increasing cybersecurity awareness in the hospice environment
Ghafir et al. (2018) <sup>12</sup>	Security threats to critical infrastructure: the human factor
Russell and Jackson (2018) <sup>13</sup>	Operating in the dark: Cyber decision-making from First Principles
Zăgan et al. (2018) <sup>14</sup>	Realities in the maritime domain regarding cybersecurity concept
Nikolova (2017) <sup>15</sup>	Best practice for cybersecurity capacity building in Bulgaria's public sector
Choi and Lee (2015) <sup>16</sup>	A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention
Rahim et al. (2015) <sup>17</sup>	A systematic review of approaches to assessing cybersecurity awareness

<sup>10</sup> Joseph Ricci, Frank Breiterger, and Ibrahim Baggili, "Survey Results on Adults and Cybersecurity Education," *Education and Information Technologies* 24 (2019): 231–249, <https://doi.org/10.1007/s10639-018-9765-8>.

<sup>11</sup> Tim Clifton, "P-236: Increasing Cyber Security Awareness in the Hospice Environment," *BMJ Supportive & Palliative Care* 8, no. 2 (2018): A94, <https://dx.doi.org/10.1136/bmjspcare-2018-hospiceabs.261>.

<sup>12</sup> Ibrahim Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," *The Journal of Supercomputing* 74 (2018): 4986-5002, <https://doi.org/10.1007/s11227-018-2337-2>.

<sup>13</sup> Scott Russell and Craig Jackson, "Operating in the Dark: Cyber Decision-Making from First Principles," *Journal of Information Warfare* 17, no. 1 (2018): 1-15, [https://cacr.iu.edu/files/documents/Operating\\_in\\_the\\_dark.pdf](https://cacr.iu.edu/files/documents/Operating_in_the_dark.pdf).

<sup>14</sup> Remus Zăgan, Gabriel Raicu, Radu Hanzu-Pazara, and Stănică Enache, "Realities in Maritime Domain Regarding Cyber Security Concept," *Advanced Engineering Forum* 27 (April 2018): 221-228, <https://doi.org/10.4028/www.scientific.net/AEF.27.221>.

<sup>15</sup> Irena Nikolova, "Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector," *Information & Security: An International Journal* 38 (2017): 79-92, <https://doi.org/10.11610/isij.3806>.

<sup>16</sup> Kyong-Ho Choi and Donghwi Lee, "A Study on Strengthening Security Awareness Programs based on an RFID Access Control System for Inside Information Leakage Prevention," *Multimedia Tools and Applications* 74, no. 20 (2015): 8927–8937, <https://doi.org/10.1007/s11042-013-1727-y>.

<sup>17</sup> Noor Hayani Abd Rahim et al., "A Systematic Review of Approaches to Assessing Cybersecurity Awareness," *Kybernetes* 44, no. 4 (2015): 606-622, <https://doi.org/10.1108/K-12-2014-0283>.



According to Rahim et al.,<sup>18</sup> adults may commit risky online behavior, for example, accessing private e-mails on public Wi-Fi networks, clicking on unfamiliar links, or using the same passwords for multiple online accounts. In addition, seniors tend not to be as cyber-savvy as the younger generation and exhibit more trustworthiness, which may be exploited through phishing and social engineering attacks, thus exposing their vulnerability.

### Cybersecurity Training and Education

Table 3 below lists the seven papers included in the final sample and their foci on cybersecurity training.

**Table 3. Articles that Relate to Cybersecurity Training and Education.**

Article	Topic
Yamin et al. (2020) <sup>19</sup>	Cyber ranges and security testbeds: scenarios, functions, tools, and architecture
Aaltola and Taitto (2019) <sup>20</sup>	Utilizing experiential and organizational learning theories to improve human performance in cyber training
Beuran et al. (2019) <sup>21</sup>	Supporting cybersecurity education and training via LMS integration: CyLMS
Raineri and Fudge (2019) <sup>22</sup>	Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs
Chapman et al. (2017) <sup>23</sup>	Can a network attack be simulated in an emulated environment for network security training?

<sup>18</sup> Rahim et al., "A Systematic Review of Approaches."

<sup>19</sup> Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers and Security* 88 (January 2020), 101636, <https://doi.org/10.1016/j.cose.2019.101636>.

<sup>20</sup> Kirsi Aaltola and Petteri Taitto, "Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training," *Information & Security: An International Journal* 43, no. 2 (2019): 123-133. <https://doi.org/10.11610/isij.4311>.

<sup>21</sup> Razvan Beuran et al., "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS," *Education and Information Technologies* 24 (2019): 3619-3643, <https://doi.org/10.1007/s10639-019-09942-y>.

<sup>22</sup> Ellen M. Raineri and Tamara Fudge, "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs," *Journal of Higher Education Theory and Practice* 19, no. 4 (2019): 73-92, <https://doi.org/10.33423/jhetp.v19i4.2203>.

<sup>23</sup> Samuel Chapman et al., "Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?" *Journal of Sensor and Actuator Networks* 6, no. 16 (2017), <https://doi.org/10.3390/jsan6030016>.

Adams and Makramalla (2015) <sup>24</sup>	Cybersecurity skills training: an attacker-centric gamified approach
Lester (2010) <sup>25</sup>	A practical application of software security in an undergraduate software engineering course

Results show that cybersecurity, in most cases, becomes compromised due to human errors and inadequate cybersecurity awareness and skills. With cybersecurity becoming a pressing issue in modern society by affecting businesses, personal life, and critical infrastructures, there is a growing need for proficiently cyber-trained personnel to protect these systems.

Topham and colleagues<sup>26</sup> reason that the organizations aiming to prepare adequately to withstand threats that can compromise their security and continuity of operations must secure every critical element of their infrastructure. The foundation starts with users who, as results indicate, are often established as the weakest link due to not being educated in cyber threats concepts and not having the experience to mitigate cyber threats that may arise. Social engineering and phishing are the most common attacks end users usually encounter. With no prior relevant training in cybersecurity, these users can rarely distinguish between a legitimate request and a cyberattack. As a result, they may inadvertently leave their company network vulnerable to threat actors. The results raise the recommendation to invest in cybersecurity awareness programs and cyber training to deal with cyber threats. Ghafir et al.<sup>27</sup> see that a challenge in implementing cybersecurity training and education in organizations is knowing how to properly provide training that will effectively engage staff (who are not ICT personnel) to practice security awareness and develop their cyber skills. For ICT professionals, the challenge is to become more proficient in analyzing and managing the constantly evolving cyber threats.

Adams and Makramalla<sup>28</sup> note that the main obstacle affecting personnel from learning how to apply security measures and establish cybersecurity skills stems from the instruction they receive from cybersecurity education programs. Most of these programs teach security concepts in a traditional approach, where it may be challenging to retain the information or put it into practice. Instead, supplementing theoretical knowledge with experiential learning and interactive

<sup>24</sup> Mackenzie Adams and Maged Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," *Technology Innovation Management Review* 5, no. 1 (January 2015): 5-14, <http://doi.org/10.22215/timreview/861>.

<sup>25</sup> Cynthia Y. Lester, "A Practical Application of Software Security in an Undergraduate Software Engineering Course," *International Journal of Computer Science Issues* 7, no. 3 (May 2010): 1-9.

<sup>26</sup> Luke Topham et al., "Cyber Security Teaching and Learning Laboratories: A Survey," *Information & Security: An International Journal* 35, no. 1 (2016.): 51-80, <https://doi.org/10.11610/isij.3503>.

<sup>27</sup> Ghafir et al., "Security Threats to Critical Infrastructure."

<sup>28</sup> Adams and Makramalla, "Cybersecurity Skills Training."

training (e.g., games, puzzles, scenarios) for general employees could provide more practical hands-on training that looks at real situational threats (e.g., via cyber ranges). Cybersecurity training programs, run by the organizations' own ICT professionals, can effectively optimize the development of cybersecurity skills and security awareness in employees so that they can competently defend themselves and organizational assets against attacks.

According to Topham et al.,<sup>29</sup> practical training through network simulated exercises and interactive cyber lab training can be beneficial in developing relevant cyber skills for students learning cybersecurity training in higher education. This may make them desired by companies when they enter the workplace as cyber-savvy employees and even future cyber professionals with competencies to deal with current and future cyber threats as ICT technology continues to advance.

### ***E-learning***

Table 4 below provides an overview of the five papers that focus on e-learning. E-learning was seen as an essential asset for organizations to invest in to achieve optimal business and individual performance in all their activities centered around ICT technology. This entails the provision of e-learning programs that develop e-skills and education necessary to use modern ICT-based devices, networks, and systems efficiently.

One of the most popular methods for e-learning, mentioned by Annansingh and Bright,<sup>30</sup> is web-based e-learning, where resources are distributed through web-based platforms and are accessible on any computer system connected to the Internet. Some benefits associated with web e-learning are remote accessibility, being able to work on courses at any location and time, possibilities for interactive training by, for example, practical applications that focus on situational instances, as opposed to instructor-led training that uses lectures in teaching security concepts, and the ability to repeat previous courses to absorb the concepts more thoroughly. Lastly, information from web-based e-learning is better retained compared to traditional training.

As many benefits are exhibited through e-learning, one obstacle that presents a challenge of taking advantage of e-learning involves having essential ICT skills. Employees with limited ICT skills may not be able to digest the information adequately, compared to others more used to working with and skillful in ICT. Some barriers that were noted are the lack of adequate time to devote to e-learning, resistance to change regarding preference in training (contact instructor-led training vs. online training), and maintaining discipline while participating in longer e-learning courses. All these reasons may result in drop-outs as courses lengthen. Having prior negative experiences in e-learning courses may also hinder success.

---

<sup>29</sup> Topham et al., "Cyber Security Teaching and Learning Laboratories."

<sup>30</sup> Annansingh and Bright, "Exploring Barriers to Effective e-Learning."

**Table 4. Articles that Relate to E-learning.**

Article	Topic
Iqbal (2016) <sup>31</sup>	Design and emergence of a pedagogical online InfoSec Laboratory as an ensemble artefact
Topham et al. (2016) <sup>32</sup>	Cybersecurity teaching and learning laboratories: a survey
Hagen et al. (2011) <sup>33</sup>	The long-term effects of information security e-learning on organizational learning
Annansingh and Bright (2010) <sup>34</sup>	Exploring barriers to effective e-learning: Case study of DNPA
Anonymous (2010) <sup>35</sup>	E-learning at Dartmoor National Park Authority: How to minimize drop-out rates and resistance to future training programs

Annansingh and Bright<sup>36</sup> recommend that to deliver successful e-learning courses, consideration must be given to the needs of the e-learner. The success of e-learning programs is determined, on the one hand, on how the course is implemented and, on the other, on the recipient. The weaknesses of the e-learner may prevent the employee from participating and benefitting in e-training. Results indicate that creating incentives (e.g., promotion or increased salary) may better encourage employees to embrace e-learning training.

### **E-skills**

As seen in Table 5 below, the final sample included only one paper that discusses the term e-skills.

<sup>31</sup> Sarfraz Iqbal, "Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact," *Journal of Information Systems Education* 27, no. 1 (2016.): 17-35, <https://aisel.aisnet.org/jise/vol27/iss1/2>.

<sup>32</sup> Topham et al., "Cyber Security Teaching and Learning Laboratories."

<sup>33</sup> Janne Hagen, Eirik Albrechtsen, and Stig Ole Johnsen, "The Long-term Effects of Information Security e-Learning on Organizational Learning," *Information Management & Computer Security* 19, no. 3 (2011): 140-154, <https://doi.org/10.1108/0968522111153537>.

<sup>34</sup> Fenio Annansingh and Ali Bright, "Exploring Barriers to Effective e-Learning: Case Study of DNPA," *Interactive Technology and Smart Education* 7, no. 1 (2010): 55-65, <https://doi.org/10.1108/17415651011031653>.

<sup>35</sup> Anonymous, "E-learning at Dartmoor National Park Authority: How to Minimize Drop-out Rates and Resistance to Future Training Programs," *Development and Learning in Organizations* 24, no. 6 (2010): 20-22, <https://doi.org/10.1108/14777281011084720>.

<sup>36</sup> Annansingh and Bright, "Exploring Barriers to Effective e-Learning."

As discussed by Singh,<sup>37</sup> the world develops into a more ICT-oriented society, and developing general ICT skills (e-skills) becomes necessary. Due to the prevalent influence ICT has on social and personal life, E-skills are essential in modern society. Investing in ICT / e-skills can provide many advantages, and cyber skills create the competence and possibilities to protect oneself against cyber threats.

**Table 5. Articles that Relate to E-skills.**

Article	Topic
Singh (2012) <sup>38</sup>	Developing e-skills for competitiveness, growth, and employment in the 21st century

## Conclusions

The academic literature primarily discusses current cybersecurity issues, such as cyber threats, cyber-related training and qualifications, and training. It is suggested to invest in studies defining what e-skills, in addition to the necessary cybersecurity-related skills, are needed to operate in modern society effectively. Four major categories regarding e-skills emerge as results of this study. As seen in Table 6, these categories serve to understand the role of cyber and e-skills in modern society. It becomes apparent that users, be they private citizens, working professionals, or ICT / cyber experts, are a potential weak link regarding cyber issues. Thus, cyber skills are needed to protect people, organizations, and society against disruptive cyber incidents and malicious cyberattacks.

Cybersecurity awareness programs that accommodate all audiences with varying degrees of e-skills and cyber knowledge can help people invest more in cultivating cybersecurity culture, with proper online behavior and a mindset towards online protection. Furthermore, such a security awareness platform could be complemented by delivery methods that effectively address cybersecurity issues and topics related to cyber threats while simultaneously improving the understanding of cyberattacks. By implementing these countermeasures of cybersecurity awareness, people can become more inclined to embrace cybersecurity awareness and be prepared to practice security measures when connected online, facilitating safer behavior in cyberspace and positive societal impacts.

When users have difficulties distinguishing between legitimate requests and possible cyberattacks, there is a gap in providing relevant cybersecurity training. Therefore, investing in cybersecurity awareness programs and cyber training to deal with cyber threats should be organizations' priority.

---

<sup>37</sup> Singh, "Developing e-Skills for Competitiveness."

<sup>38</sup> Singh, "Developing e-Skills for Competitiveness."

**Table 6. Main Findings.**

Category	Main Findings
General Cybersecurity	<ul style="list-style-type: none"> <li>• cyber devices vulnerable to cyberattacks</li> <li>• people are either not knowledgeable in cybersecurity or fail to practice cybersecurity measures</li> </ul>
Cybersecurity Training and Education	<ul style="list-style-type: none"> <li>• end-users often considered as the weakest link</li> <li>• recommendation to invest in cybersecurity awareness programs and cyber training</li> <li>• practical training through network simulated exercises and interactive cyber lab training can be beneficial</li> </ul>
E-learning	<ul style="list-style-type: none"> <li>• e-learning as an essential asset for organizations to invest in</li> <li>• benefits of web-based e-learning: remote accessibility, work at any location/time, interactive training possible</li> </ul>
E-skills	<ul style="list-style-type: none"> <li>• modern society has gradually become more technology driven</li> <li>• the development of e-skills training has become essential</li> <li>• e-skills pertain to activities of both business people and or casual users</li> <li>• benefits of developing e-skills are extensive on a personal level</li> </ul>

As ICT has become a critical factor in establishing global competitiveness, growth, and innovation in Europe, it is necessary to invest in e-skills education and cybersecurity training in order to develop resilient societal, economic, and industrial systems. Governments and academic institutions could help various organizations address shortages in ICT competence in the workplace by facilitating cyber skills training courses and education in e-skills, thus continually cultivating growth and innovation in the European economies through ICT developments.

In addition, to incorporate effective cybersecurity and e-skills programs, educators should address the factors preventing users from investing in these programs. Instructors may tailor their pedagogical methods and systems in ways that best benefit end-users while optimizing the enhancement of their e-skills. As a result, the learner has an engaging experience within these programs and can use the new skills for personal improvement while contributing to society.

This study shows a general lack of established IT terms. There are “e-skills,” “cyber skills,” “computer skills,” “ICT skills,” and they all can mean different things to different authors. We recommend continued research to identify clear definitions for each of these terms.

## **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

## **Acknowledgment**

This work was supported by the ECHO project, which has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement no. 830943. The European Commission-funded cyber pilot projects, such as the “European network of Cybersecurity centres and competence Hub for innovation and Operations” (ECHO), bring opportunities for researchers to conduct experiments and gather empirical data to study these aspects from different perspectives.

## **About the Authors**

**Harri Ruoslahti**, PhD, is a Senior Lecturer in Security and Risk Management of the Laurea University of Applied Sciences. He also leads Laurea’s team in the Horizon 2020 project “European network of Cybersecurity centres and competence Hub for innovation and Operations” (ECHO).  
E-mail: harri.ruoslahti@laurea.fi

**Janel Coburn** worked as Research, Development, and Innovations Expert at Laurea University of Applied Sciences, where she contributed to several RDI projects, including the study of cyber skills in the ECHO project.

**Amir Trent** was a BSc student in Business Information Technology at Laurea University of Applied Sciences.

**Ilkka Tikanmäki** is a researcher in Security and Risk Management at the Laurea University of Applied Sciences and a doctoral student of Operational art and tactics at the Finnish National Defence University.







# Disinformation: Policy Responses to Building Citizen Resiliency

*Inez Miyamoto*

*Daniel K. Inouye Asia Pacific Center for Security Studies*

**Abstract:** Maligned actors use fake social media accounts and automated tools, also called computational propaganda, to launch disinformation operations. While technology companies and researchers continue to advance computational propaganda detection, they also know that eradicating social bots and disinformation is impossible. Since computational propaganda continues to increase, governments need to focus their efforts on developing policies that decrease citizen demand for disinformation. The purpose of this article is to explore disinformation at the intersection between technology and citizen resiliency. First, the current landscape will be explored to understand the impact of disinformation on society and its citizens. Second, the effect of technology on the supply of disinformation will be examined. Third, methods to decrease the demand for disinformation will be considered to increase citizen resiliency.

**Keywords:** disinformation, digital literacy, citizen resilience.

## Introduction

With the growth of social media, there is a flood of unregulated content available on the Internet. Gone are socially-responsible publishers, editors, and subject matter experts to evaluate information that was available with traditional media.<sup>1</sup> Instead, citizens are left to decide what is fake or real, while maligned actors leverage this opportunity, along with the openness of democracies, to influence societies with disinformation. Disinformation is defined as the purposeful use of

<sup>1</sup> Institute for the Study of Diplomacy, *The New Weapon of Choice: Technology and Information Operations Today* (Washington: Institute for the Study of Diplomacy, October 2020), <https://georgetown.app.box.com/s/ivwz4irk3un8blngm3wo0t3uwfc6hpz8>.

false information created and spread intentionally as a way to confuse or mislead, which may contain a blend of truth and untruth or purposefully exclude context.<sup>2</sup> Governments need to focus their efforts on developing policies to decrease citizen demand for disinformation because controlling the supply of disinformation is a formidable task when machines are increasingly creating the content.

Governments, civil society groups, and technology companies recognize disinformation as a global problem, but they struggle with their responses. Malign actors sow discord and distrust using newer and better tools, leaving citizens, who are the target of disinformation operations, worried about the impact of disinformation on the Internet. Knuutila and colleagues found that 53% of regular internet users (154,195 respondents in 142 countries) were concerned about encountering disinformation online, with the highest concern (65%) coming from North America.<sup>3</sup> They were more concerned about disinformation than online fraud or harassment.

This article examines disinformation at the intersection between technology and citizen resiliency. First, the current landscape will be explored to understand the impact of disinformation on society and its citizens. Second, after examining the impact of technology on the supply-side of disinformation, the demand-side of disinformation is examined for citizen resiliency. Finally, this article concludes with policy recommendations for starting a citizen resiliency program.

## Computational Propaganda

Malign actors use fake social media accounts and automated tools, also called computational propaganda, to launch disinformation operations. Woolley and Howard (2016) define computation propaganda as “algorithms, automation, and human curation to purposefully distribute misleading information over social media networks.”<sup>4</sup> As an illustration, the computational propaganda tools include bots, sock puppets, robo-trolls, and deepfake videos.

First, bots—short for robots—are software programs with legitimate uses, such as automating tasks on websites. In disinformation operations, social media bots impersonate a human on social media by communicating and interacting

---

<sup>2</sup> Samantha Bradshaw and Lisa-Maria Neudert, “The Road Ahead: Mapping Civil Society Responses to Disinformation,” Working Paper (Washington: National Endowment for Democracy, January 2021), <https://www.ned.org/mapping-civil-society-responses-to-disinformation-international-forum>.

<sup>3</sup> Aleksi Knuutila, Lisa-Maria Neudert, and Philip N. Howard, “Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries,” COMPROP Data Memo 2020.8, December 15, 2020, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2020/12/Global-Fears-of-Disinformation-v.13.pdf>.

<sup>4</sup> Samuel C. Woolley and Philip N. Howard, “Automation, Algorithms, and Politics: Political Communication, Computational Propaganda, and Autonomous Agents – Introduction,” *International Journal of Communication* 10 (2016), <https://ijoc.org/index.php/ijoc/article/view/6298>.

with people and systems. For example, they can be social bots, which are fake, automated accounts, or cyborgs, which are accounts operated by a human with bot technology assistance. Malign actors also use a massive number of social media bots to create the illusion of large-scale consensus for online propaganda.<sup>5</sup>

Second, sock accounts or sock puppets are fictitious online accounts created by an individual or group with an intent to deceive. For example, an individual or group will create multiple accounts on a social media platform to influence social media by generating followers by “liking” or voting on posts. They can also slant or distort an online discussion or support a particular online account. As a case in point, Russian intelligence operated a Twitter sock account under the name of Jenna Abrams, which had 70,000 followers, to influence conservative voters during the 2016 US elections.<sup>6</sup>

Third, trolls are real individuals who intentionally provoke others online by posting inflammatory or offensive messages. When their accounts are automated through the use of software, they are called robo-trolls and are capable of generating content.<sup>7</sup> Researchers are concerned about the use of robo-trolls by extremists or terrorists. Therefore, they are testing text-generating artificial intelligence (AI) software, which could be used in the future by robo-trolls.<sup>8</sup> The text-generating AI software would be a powerful tool for extremists or terrorists because they could speedily create propaganda, which at present is manually created by humans and thus a time-intensive process.

Fourth, AI-enabled tools allow the creation of deepfake videos – digitally altered videos used for deceptive purposes. According to Sensity AI (formerly DeepTrace), the amount of deepfake videos is increasing, with 96% of online deepfake videos consisting of non-consensual, celebrity pornography.<sup>9</sup> Experts believe these videos will continue to grow in numbers and sophistication as more

---

<sup>5</sup> Samuel C. Woolley and Philip N. Howard, “Computational Propaganda Worldwide: Executive Summary,” Working Paper No. 2017.11 (Oxford: University of Oxford, 2017), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>.

<sup>6</sup> Ben Collins and Joseph Cox, “Jenna Abrams, Russia’s Clown Troll Princess, Duped the Mainstream Media and the World,” *The Daily Beast*, November 3, 2017, <https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world>.

<sup>7</sup> Tom Simonite, “To See the Future of Disinformation, You Build Robo-Trolls: AI-Powered Software Is Getting Better and Could Soon Be Weaponized for Online Disinformation,” *Wired*, November 19, 2019, <https://www.wired.com/story/to-see-the-future-of-disinformation-you-build-robo-trolls>.

<sup>8</sup> Simonite, “To See the Future of Disinformation, You Build Robo-Trolls.”

<sup>9</sup> Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, *The State of Deep-fakes: Landscape, Threats and Impact* (Amsterdam: Deepttrace, 2019), <https://sensity.ai/reports/>.

deepfake services and tools become available to the public.<sup>10</sup> Even now, high-quality deepfake videos are difficult to detect.<sup>11</sup>

In response to increasing computational propaganda, technology companies began deploying AI-enabled countermeasures. As companies became better at detecting and blocking bots, bot developers began using more sophisticated techniques, such as AI-generated images, text, and videos.<sup>12</sup> In view of the fact that synthetically-generated content mimics a human's style, distinguishing AI content from human-generated content is challenging.<sup>13</sup> And recent social bots are more similar to human-operated accounts because AI is being used to create a hybrid of automated and human-driven behaviors."<sup>14</sup> Compounding this problem is the fact that malign actors are able to weave true information with false information, making it even more difficult for technology companies to label disinformation as truthful or untruthful.<sup>15</sup> Consequently, in the future, it will be impossible for citizens to determine the veracity of information or legitimacy of accounts.

Meanwhile, computation propaganda is increasing globally. Bradshaw et al. noted that state and political actors in 81 countries are using social media to spread computational propaganda.<sup>16</sup> This increase is problematic because computational propaganda is a "powerful tool that can undermine democracy."<sup>17,18</sup> While technology companies and researchers continue to advance computational propaganda detection, they also know that eradicating social bots and disinformation is impossible. Instead, a whole-of-society approach is necessary to build citizen resilience against a growing threat that is undermining societal trust.

---

<sup>10</sup> Ajder, Patrini, Cavalli, and Cullen, *The State of Deepfakes*.

<sup>11</sup> Matt Groh, "DetectDeepFakes: How to Counteract Misinformation Created by AI," accessed January 28, 2021, [www.media.mit.edu/projects/detect-fakes/overview](http://www.media.mit.edu/projects/detect-fakes/overview).

<sup>12</sup> Stefano Cresci, "A Decade of Social Bot Detection," *Communications of the ACM* 63, no. 10 (October 2020): 72-83, <https://doi.org/10.1145/3409116>.

<sup>13</sup> Renée DiResta, "The Supply of Disinformation Will Soon Be Infinite: Disinformation Campaigns Used to Require a Lot of Human Effort, but Artificial Intelligence Will Take Them to a Whole New Level," *The Atlantic*, September 20, 2020, <https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400>.

<sup>14</sup> Cresci, "A Decade of Social Bot Detection."

<sup>15</sup> Kate Starbird, "Disinformation's Spread: Bots, Trolls, and All of Us," *Nature* 571, no. 449 (2019), <https://doi.org/10.1038/d41586-019-02235-x>.

<sup>16</sup> Samantha Bradshaw, Hannah Bailey, and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: University of Oxford, 2021), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf>.

<sup>17</sup> Woolley and Howard, "Computational Propaganda Worldwide."

<sup>18</sup> Stanford History Education Group (SHEG), "Evaluating Information: The Cornerstone of Civic Online Reasoning," Working Paper (Stanford: SHEG, 2016), <https://stacks.stanford.edu/file/druid:fv751yt5934/SHEG%20Evaluating%20Information%20Online.pdf>.

Governments are responding to disinformation from both sides of the supply-demand equation. The supply-side of disinformation involves limiting the flow of disinformation into the information ecosystem. The demand-side involves addressing citizen consumption of disinformation.<sup>19</sup> Next, this article explores both sides of the supply-demand equation of disinformation.

## **Supply-Side of Disinformation**

Without a doubt, tackling the supply-side of disinformation necessitates the government, technology companies, and civil society to work together to develop a whole-of-society response. From a policymaker's perspective, countering supply-side disinformation is challenging because there may not be a lead agency responsible for countering disinformation operations. For this reason, a country may not have a coordinated policy response. Consequently, when there is a disinformation attack on domestic affairs (e.g., election security, disasters, pandemic response and vaccinations), the functional agency may not be equipped to respond to an attack. And, when there are overlapping equities or responsibilities, determining which government agency should lead a response may become a problem (e.g., homeland security, defense department, justice department, election authority, or another agency). Malign actors understand the seams between government agencies and leverage them to launch their attacks.

Supply-side approaches to curbing the spread of disinformation include legislation, government fact-checkers, and information troops; however, it is still too early to know which ones are most effective.<sup>20</sup> For example, in 2017, Germany passed the Network Enforcement Act, compelling social media companies to remove hate speech and other illegal content. The downside of this type of law is that it can lead to censorship and curtail free speech.<sup>21</sup>

Another supply-side approach is the European Union's implementation of a voluntary, self-regulatory standard for technology companies, such as Google, Facebook, Mozilla, and Twitter. In 2018, they signed the European Commission's Code of Practice on Disinformation and committed to increasing the transparency of political ads, closing fake accounts, and addressing the malicious use of bots. However, the preliminary report of the Code of Practice was mixed. There continues to be a lack of trust between social media companies, governments,

---

<sup>19</sup> Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," *Atlantic Council*, June 2019, [https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic\\_Defense\\_Against\\_Disinformation\\_2.0.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf).

<sup>20</sup> Olga Robinson, Alistair Coleman, and Shayan Sardarizadeh, "A Report of Anti-Disinformation Initiatives" (Oxford: University of Oxford, August 2019), <https://comprop.oxi.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives>.

<sup>21</sup> "Germany: Flawed Social Media Law," *Human Rights Watch*, February 14, 2018, <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>.

and civil society, primarily because technology companies give only limited access to their data.<sup>22</sup> In 2020, the European Commission implemented a comprehensive response to counter disinformation through the European Democracy Action Plan.<sup>23</sup> One of the initiatives is to overhaul the Code of Practice into a co-regulatory framework.

In contrast, Estonia, which has been the target of Russian disinformation since 2007, involves civil society in its approach. The government created a voluntary security force called the Estonia Defense League within the Ministry of Defense. The Estonia Defense League supports cyber defense but also monitors the Internet for disinformation and uses an anti-propaganda blog to counter distorted narratives. Estonia also involves an internet activist group called the Baltic Elves to respond to Russian trolls, report bots, provide counter-narratives.<sup>24</sup> In addition, since Estonia has a sizeable ethnic-Russian population, it operates a Russian-language television station to counter disinformation.

Taiwan is another country with a whole-of-society approach to curbing the supply-side of disinformation. Since 2018 when Taiwan appointed its first Digital Minister, the country instituted several civic-tech initiatives to build citizen and civil society trust. The Digital Minister not only developed a transparent government but also combined the efforts of government teams, technology companies, and private citizens to counter disinformation. Taiwan deployed several successful initiatives, including an Internet Fact-Checking Network, chatbots for social media fact-checking, and memes to challenge disinformation narratives.<sup>25</sup>

The greatest strength of Estonia and Taiwan's approach is the involvement of citizens in combatting disinformation. The battle against disinformation can only be won by starting with the citizens who are consuming and spreading disinformation. When the disinformation can be ignored by citizens, its spread will decrease. In the next section, this article explores methods to address the demand-side of disinformation.

---

<sup>22</sup> James Pammet, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission" (Carnegie Endowment for International Peace, March 3, 2020), <https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187>.

<sup>23</sup> European Commission, "European Democracy Action Plan," accessed February 2, 2021, [https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en).

<sup>24</sup> Joseph Robbins, "Countering Russian Disinformation" (Center for Strategic & International Studies, September 23, 2020), <https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>.

<sup>25</sup> Rory Daniels, "Taiwan's Unlikely Path to Public Trust Provides Lessons for the US," *Brookings*, September 15, 2020, <https://www.brookings.edu/blog/order-from-chaos/2020/09/15/taiwans-unlikely-path-to-public-trust-provides-lessons-for-the-us>.

## Demand-Side of Disinformation

One way to achieve demand-side reduction is through digital literacy education and disinformation awareness.<sup>26</sup> There is evidence that digital literacy can be an effective strategy to help counter disinformation.<sup>27</sup> Since there is no universal definition of digital literacy, in this article, digital literacy includes media, news, and information literacy and is defined as “the ability to use information and communication technologies to find, evaluate, create and communicate information, requiring both cognitive and technical skills.”<sup>28</sup>

A common misconception is that older citizens are more susceptible to disinformation than younger citizens because of their lack of comfort with digital technology. There is evidence that senior citizens are more likely to share disinformation using social media.<sup>29</sup> However, younger citizens, who may be more comfortable with technology, are also susceptible to disinformation because they lack digital literacy skills. The Stanford History Education Group found that middle school, high school, and college students had difficulty evaluating the credibility of social media information. They incorrectly perceived information as trustworthy based on incorrect facts: a search engine result appearing at the top, a website using the .org domain or a Twitter account with many followers.<sup>30</sup> These gaps, therefore, demonstrate a societal need for digital literacy.

Policymakers and educators are rethinking the framework of digital literacy to ensure that critical thinking and civics are included in the curriculum. In the past, governments were more focused on developing digital skills needed for “digital transformation” initiatives that did not necessarily include critical thinking and civics. However, newer programs include citizen resiliency. For example, in 2019, Canada created a Digital Citizen Initiative using a multi-stakeholder approach. The initiative supports citizen-focused activities, such as the development of learning materials, investment in research programs, and promotion of

---

<sup>26</sup> Polyakova and Fried, “Democratic Defense Against Disinformation 2.0.”

<sup>27</sup> Andrew M. Guess et al., “A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India,” *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536-15545, [www.pnas.org/content/pnas/117/27/15536.full.pdf](http://www.pnas.org/content/pnas/117/27/15536.full.pdf).

<sup>28</sup> American Library Association (ALA), “Literacy for All: Adult Literacy through Libraries,” (Chicago: ALA, 2019), [http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/Literacy%20for%20All\\_Toolkit\\_Online.pdf](http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/Literacy%20for%20All_Toolkit_Online.pdf).

<sup>29</sup> Andrew Guess, Jonathan Nagler, and Joshua Tucker, “Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook,” *Science Advances* 5, no. 1 (January 2019), <https://doi.org/10.1126/sciadv.aau4586>.

<sup>30</sup> Stanford History Education Group, “Evaluating Information: The Cornerstone of Civic Online Reasoning.”



media literacy (civic, news, and digital).<sup>31</sup> In contrast, there are also non-government-led programs. For example, two institutes located at the University of South Florida (Florida Center for Cybersecurity and the Florida Center for Instructional Technology) partnered with New America (a non-profit, non-partisan think tank) to develop cyber citizenship skills for primary and secondary students. They aim to create a Cyber Citizenship Working Group to collaborate with various civil society stakeholders and establish a Cyber Citizenship Portal to provide an educational toolkit for the public.<sup>32</sup>

It is still too soon to determine the effectiveness of the digital literacy education and awareness programs. Moreover, preparing citizens for digital literacy is only the first step to other knowledge and skillsets, such as algorithmic literacy and data literacy (as a result of AI).<sup>33</sup> For the challenges ahead, policymakers need to use strategic foresight to prepare citizens for the next-generation disinformation attacks better. In summary, the below policy recommendations are a starting point for developing citizen resiliency.

### ***Policy Recommendation #1: Improve the Digital Literacy of All Citizens***

Governments must develop a digital literacy program to educate all citizens about digital literacy by establishing a standard or framework. There are many frameworks to use as a foundation for creating a digital literacy program. They include the United Nations Educational, Scientific and Cultural Organization (UNESCO) Digital Literacy Global Framework, the European Union Digital Competence Framework for Citizens, and Dr. Yuhyun Park's Digital Intelligence (DQ) Framework.

Once the framework is developed, the government should create a digital literacy curriculum that meets the need of citizens at different stages of life (primary, secondary and tertiary levels). By developing curricula for different levels, educators and trainers can quickly adapt the material to their educational program. Methods to make the content accessible for adults include producing massive open online courses and creating online videos supporting lifelong, self-paced learning. The digital literacy skills will not only build citizen resilience to disinformation but will also prepare citizens for the impending digital transformation, which is the adoption of digital technology to transform society.

---

<sup>31</sup> UNESCO, "Digital Citizen Initiative," *UNESCO Diversity of Cultural Expressions*, accessed February 1, 2021, <https://en.unesco.org/creativity/policy-monitoring-platform/digital-citizen-initiative>.

<sup>32</sup> "Cyber Florida, Florida Center for Instructional Technology and New America Launch New Partnership to Improve 'Cyber Citizenship' Skills for K-12 Students," *New America* (International Security), December 16, 2020, [www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship](http://www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship).

<sup>33</sup> Ramesh Srinivasan, "This Is How Digital Literacy Can Transform Education," *World Economic Forum*, March 3, 2020, <https://www.weforum.org/agenda/2020/03/why-is-digital-literacy-important>.



### ***Policy Recommendation #2: Include Digital Security in Annual Cybersecurity Awareness Campaigns***

Citizen awareness begins with public awareness campaigns. Many governments already use annual cybersecurity awareness month or week to promote online safety and advocate for security practices. Since a core component of cybersecurity deals with understanding the online threats that jeopardize citizen safety, disinformation is an appropriate topic for raising awareness. For example, issues for attention could include a lesson on social bots or on evaluating the sources of online information. An awareness campaign provides yet another opportunity to sensitize citizens about disinformation.

### ***Policy Recommendation #3: Empower Civil Society by Building Trust and Sharing Information on State and Political Actors Using Computational Propaganda***

Empowering citizens by building trust and sharing information builds citizen resilience. Citizens do not understand the volume and intensity of the computational propaganda attacks against their country unless they are strengthened with information. They need to know who, what, where, when, and how disinformation attacks occur and what they can do to counter the disinformation. Since political computation propaganda attacks can be state-sponsored attacks, the government may not fully share the details of an attack due to classification reasons. To achieve trust, governments must find a way to be transparent about the attacks while balancing the need for security. Also, when sharing information, plain language should be used, omitting technical and government jargon.

Governments can also foster public-private partnerships to share information and collaborate to solve the technical computational propaganda and citizen resiliency challenges. In view of the fact that technology companies possess the data that government, civil society groups, and researchers need to develop countermeasures, the partnership provides an opportunity to create innovative solutions through crowdsourcing and trust through information sharing and open dialogue. Now, more than ever, government, technology companies, and civil society must work together to build collective trust and citizen resiliency.

### **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

### **About the Author**

**Inez Miyamoto** is a cybersecurity professor at the Daniel K. Inouye Asia Pacific Center for Security Studies. E-mail: [miyamotoi@dkiapcss.net](mailto:miyamotoi@dkiapcss.net)





## Social Media – Hate Speech – Hate Crime

**Lukáš Vilím**

*Ministry of the Interior of the Czech Republic, <https://www.mvcr.cz/mvcren/>*

**Abstract:** This article examines the issue of hate speech on social media from the perspective of the security system of the Czech Republic and its tools designed to provide internal security and the necessary legislative amendments to allow law enforcement agencies to address this issue effectively. In the current approach to cyberspace, social networks are becoming a vehicle for the persistent spreading of hate-based ideologies, and this needs to be prevented.

**Keywords:** social network, security system, hate speech, criminal activity, extremism, terrorism, prevention.

### Introduction

Nowadays, it is not uncommon for social media to include manifestations of hatred, misleading information, and elements of extremism or terrorism. We already observe that political and religious extremist groups use social media and networks to promote their ideology, recruit new members, demonstrate their power, and shock society with videos of wars as something commonplace and unavoidable. Society is already able to act against such use of social networks and its negative consequences. There are many ways to do so. First of all, social media or network users can react and point out inappropriate behavior in their circle of friends and state that they do not wish to be part of similar posts. They can condemn such behavior or remove such profiles from their circle of friends. We may call this approach naive, but we will assume that we are in a democratic society built on a collective agreement between the citizens, which implies a certain moral responsibility to those around us. Another way is to report the problematic profile to the social media or network administrator, who will assess whether the level of violence or hatred in the post is so significant that intervention in the form of blocking and deleting the account is needed. In extreme cases,

it is possible to decide on legal steps, namely to report inappropriate comments, profiles, or groups to law enforcement agencies (*orgány činné v trestním řízení – OČTŘ*), whose duty is to assess whether the conditions that classify an act as a crime have been fulfilled and whether it is necessary to follow the appropriate steps according to the Criminal Procedure Code.

Before paying attention to repressive steps, it is necessary to focus on the tools available in a democracy and its security system within the Czech Republic to successfully combat this phenomenon in the real world and the cyberworld.

## **Tools of the Security System of the Czech Republic Designed to Deal with Hate Speech on the Internet**

A democratic state is governed by its constitution and the Charter of Fundamental Rights and Freedoms that guarantee freedom of expression. It must have adequate tools in place to guarantee such rights and, at the same time, prevent undesirable displays and trespasses against the law in their exercise. The issue of hate speech or the deliberate publication of misleading news can be explored from several angles: from the point of view of the internal security of the state, the ethical education of society, the professionalism of the media, or the security forces of the state.

The top of the security system is formed by the government, executive departments, and the Chamber of Deputies of the Czech Republic. The permanent working body of the Government of the Czech Republic for resolving issues in the field of security is the State Security Council (*Bezpečnostní rada státu – BRS*), the existence of which is enshrined in the Constitutional Act No. 110/1998 Coll., *On the Security of the Czech Republic*. It can be one of the strategic tools for addressing new threats present in cyberspace in the form of objectionable content. According to the statute,<sup>1</sup> the BRS has six permanent working bodies tasked to submit strategic documents and materials addressing the security of the state (i.e., new security threats). The security of cyberspace is examined at three basic levels: cyber defense, cyber security, and cybercrime. Institutionally, cybersecurity is based on effective and coordinated activities of the armed forces, the relevant office for cyber security (National Cyber and Information Security Agency; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), security forces (especially the Police of the Czech Republic), and intelligence services, but also the private sector. Due to this possible division of the issue, in solving the problem of hate speech in cyberspace, three BRS committees come into consideration: The Committee on Internal Security (falling under the responsibility of the Ministry of the Interior), the Committee on Cyber Security (under the responsibility of the National Cyber and the Information Security Agency), and the Committee on Intelligence under the Prime Minister. So far, all efforts to address

---

<sup>1</sup> Government of the Czech Republic, <https://www.vlada.cz/assets/ppov/brs/Statut-BRS-rijen-2018.pdf>.

hateful content or misleading messages in cyberspace have been primarily submitted to the Committee on Internal Security, which is the correct procedure according to the Competence Law.<sup>2</sup>

The existence and danger of hate speech on the internet were reported as early as 1997 by the “Report on the Progress of State Authorities in Prosecuting Crimes Motivated by Racism and Xenophobia” (“Zpráva o postupu státních orgánů při postihu trestných činů motivovaných rasismem a xenofobií”) and subsequently with greater intensity by each new annual report on extremism and terrorism issued by the Ministry of the Interior. From the content of the individual reports, it is possible to conclude that the internet environment and subsequently the environment of social media and networks become not only a venue for spreading hateful ideas or extremist ideologies but also an environment of hate speech and direct attacks on people because of their color, religion, or merely differing opinions. For this reason, more emphasis is placed on monitoring events on the internet related to extremism and terrorism, which can be read in the respective annual reports by the police authorities, intelligence services, and academics.

The issue of hate crime and hate speech is addressed in a document prepared by Prof. Miroslav Mareš in 2011 in an analysis entitled “*Problematika Hate Crime*” (“The Issue of Hate Crime”). This analysis mentioned the commitment

to take action against all forms of expression, including in the media and on the internet, which may reasonably be construed as bringing the result of inciting, spreading, or supporting discrimination against lesbian, gay, bisexual, and transgender people, and other forms of discrimination. Such displays should be prohibited and publicly condemned whenever they occur. All measures should respect the fundamental rights to freedom of expression in accordance with Article 10 of the Convention and the judicature of the Court of Justice (Committee of Ministers, Council of Europe 2010).<sup>3</sup>

This is precisely the effort to address the issue of hate speech on the internet, including on social networks, at the international level.

The so-called “National Security Audit” (“Audit národní bezpečnosti”), which addresses the phenomenon of hateful content on the internet in several chapters, can undoubtedly be considered an important material of the Ministry of the Interior in relation to dealing with the issue. The issue of combating the spread of hateful and radical content on the internet and social media is addressed in

---

<sup>2</sup> Act No. 2/1969 Coll., “On the Establishment of Ministries and Other Central Bodies of the State Administration of the Czech Republic, Which Designates Individual Central Bodies and Regulates Their Competence,” Public administration portal, Ministry of Interior, <https://portal.gov.cz/app/zakony/zakonPar.jsppage=0&idBiblio=31338&fulltext=&nr=2~2F1969&part=&name=&rpp=15#local-content>.

<sup>3</sup> “Problematika Hate Crimes,” Home page of the Ministry of the Interior of the Czech Republic Ministerstvo vnitra České republiky, accessed July 20, 2020, [www.mvcr.cz/clanek/problematika-hate-crimes.aspx](http://www.mvcr.cz/clanek/problematika-hate-crimes.aspx).

the chapter on terrorist threats, on extremist threats, both right-wing (e.g., hatred of certain minority groups) and left-wing (class hatred, hatred of ideological opponents, and hatred of state power and the whole democratic system), threats consisting of disinformation campaigns that use the spread of hatred against certain groups of the population, as well as state authorities, or the direction of the foreign policy of the Czech Republic to achieve military, political, or economic objectives. The audit also describes cyber terrorism as a real security threat when the state has an obligation, *inter alia*, to defend itself against activities in cyberspace in the form of incitement to hatred or the creation and spread of propaganda. The cyber environment concerning terrorism must be understood as a means or an instrument for achieving the attacker's political, religious, or other ambitions.<sup>4</sup> The National Security Audit, as important security and strategic document, was approved by Government Resolution No. 1125 of December 14, 2016, and passed the commenting procedure of the Committee for Internal Security and subsequently the State Security Council. The government resolution instructed the Minister of the Interior to draw up an Action Plan for the National Security Audit and submit it to the government by April 30, 2017. The action plan was approved by the Government's Resolution No. 407 of May 22, 2017. At the same time, the managers of the individual measures of the Action Plan were instructed to ensure their implementation. For example, the Minister of the Interior was instructed to submit an evaluation of the implementation of the Action Plan to the State Security Council by April 30 of each year.<sup>5</sup> The State Security Council took note of the evaluation of the implementation of the National Security Audit Action Plan for 2019 by a resolution of June 8, 2020. The material contained a clear summary of the status of tasks assigned to individual managers, which also applies to the issue of hate speech.<sup>6</sup>

As mentioned above, the State Security Council or some of its committees must directly pay attention to the issue of hate speech. In addition to the Committee on Internal Security (*Výbor pro vnitřní bezpečnost – VVB*), which is a key and main platform for this issue, other committees may address this phenomenon as well if it is relevant to them and fulfills the purpose for which they were established.

---

<sup>4</sup> "Audit národní bezpečnosti – Bezpečnostní aspekty migrace – Aktuální informace o migraci," Ministry of the Interior of the Czech Republic, accessed July 21, 2020, <https://www.mvcr.cz/migrace/clanek/audit-narodni-bezpecnosti-bezpecnostni-aspekty-migrace.aspx>.

<sup>5</sup> Resolution of the Government of the Czech Republic of December 14, 2016, No. 1125.

<sup>6</sup> "Bezpečnostní rada státu se zabývala otázkami spojenými s řešením situace v souvislosti s výskytem onemocnění covid-19," Government of the Czech Republic, June 8, 2020, <https://www.vlada.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-se-zabyvala-otazkami-spojenymi-s-resenim-situace-v-souvislosti-s-vyskytem-onemocneni-covid-19-181915/>.

Hate speech can also be part of media disinformation campaigns, currently referred to as *fake news*<sup>7</sup> – false news in social media and networks, often abused by extremists to promote their ideas. Society has long demanded that this phenomenon is also addressed at the political level. It also potentially requires that the relevant authorities comment on individual false campaigns. In addressing this security threat, it is essential to realize that the state and public central administration bodies do not have a monopoly on the truth and cannot comment on media reports in the “this is true, and this is false” way. Before a news item is marked as false, it must be analyzed, and it must be determined which information that makes up the specific “fake news” is to be marked as false. In this respect, democratic society has its own independent media, which verify the reports, criticize them, and then comment on them. Public authorities can only comment on a piece of news if they have enough verified information and if it is within the framework of the issues they manage. Then the citizens will form a particular picture and decide whether they will believe the news or consider it untrue.

Displays of hatred, which is a part of false news or commentaries on social media or networks, can also be part of political campaigns of states, the intention of which is to influence the citizens of the country, state policy, or to divert attention from real problems. The combination of multiple threats to the integrity and unity of the state is a current trend, referred to as a hybrid threat. This term is often used, but defining its content is not that simple:

The definitions of hybrid threats vary, responding to the changing nature of these threats. In general, [a hybrid threat] is a set of different coercive and subversive activities and conventional and unconventional methods (e.g., diplomatic, military, economic and technological) that various state and non-state actors can use in a coordinated way to achieve specific goals without formally declaring war. The aim is usually to exploit the vulnerabilities of the target and to create confusing situations in order to disrupt decision-making processes. *Massive disinformation campaigns and the use of social media for propaganda or for radicalization, recruitment and direct control of supporters* can be tools of these hybrid threats.<sup>8</sup>

To counter hybrid threats, the Ministry of the Interior has set up a so-called Center for Terrorism and Hybrid Threats (*Centrum pro terorizmus a hybridní hrozby* – CTHH), whose task is to “address hybrid threats affecting the security of the Czech Republic and at the same time falling within the sphere of the Ministry of the Interior, such as terrorism, attacks on soft targets, security aspects of

---

<sup>7</sup> Fake news is *false news*. The term refers to alarming *hoaxes*, false information and misinformation that spreads on the internet, in the print media and on television. People often encounter it for example on social media and networks or in emails. Source: *nav-heck*, July 23, 2020, <https://www.vodafone.cz/uzitecne-odkazy/slovník-pojmu/fake-news/>.

<sup>8</sup> “Hybridní hrozby,” Ministry of Health, last updated July 20, 2020, [www.mzcr.cz/hybridni-hrozby](http://www.mzcr.cz/hybridni-hrozby).

migration, *extremism*, mass events, disturbance of public order and various criminal activity, or security aspects of *disinformation campaigns related to the internal security of the state*. The center was established on the basis of the recommendations of the National Security Audit approved by the government.”<sup>9</sup> CTHH was established by the decision of the Minister of the Interior Milan Chovanec, as of January 1, 2017, based on the National Security Audit and following the 2015 Security Strategy of the Czech Republic.<sup>10</sup>

The State Security Council also responded by establishing *an expert working group for hybrid threats*. The group includes representatives of the State Security Council, the intelligence services of the Czech Republic, the National Security Office, the Police of the Czech Republic, the Czech National Bank, the State Office for Nuclear Safety, and the Government Commissioner for Cyber Security. This expert working group was established by the Resolution of the State Security Council No. 9 of March 8, 2017, obligating all its members to cooperate in exchanging information on hybrid threats.<sup>11</sup>

As described above, the state has many tools at its disposal to address hate speech, even at the highest governmental level. It is up to members of the government or the State Security Council to decide whether they find hate speech of such concern as to address it by adopting adequate countermeasures or leave the response to lower-level institutions such as law enforcement agencies dealing with cybercrime. On the other hand, it is necessary to realize that lower levels have an obligation to submit suggestions and proposals to address new security threats. The task of the manager for internal security is, therefore, to monitor and evaluate information from their units and develop counter-strategies. It is also important to realize that addressing the issue of hate speech by organized extremist groups, for example, is the responsibility of the Ministry of the Interior, along with other security forces that may also submit conceptual and strategic materials to committees of the State Security Council.

## Current Legislation Addressing Hate Speech on Social Media

We do not find a definition of hate speech in the Czech legal system:

It is usually understood as a type of offensive speech that incites, encourages or spreads hatred towards a certain group of persons or an individual and is often provoked by prejudices and stereotypes. The reason for hatred can be,

<sup>9</sup> “Úvodní strana – Terorismus a měkké cíle,” Ministry of the Interior of the Czech Republic, accessed July 24, 2020, <https://www.mvcr.cz/cthh/>.

<sup>10</sup> “Bezpečnostní strategie České republiky,” Government of the Czech Republic, 2015, accessed October 9, 2020, <https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf>.

<sup>11</sup> “Bezpečnostní rada státu schválila ustavení odborné pracovní skupiny pro hybridní hrozby,” Government of the Czech Republic, March 8, 2017 [www.vlada.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-schvalila-ustaveni-odborne-pracovni-skupiny-pro-hybridni-hrozby-154226/](http://www.vlada.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-schvalila-ustaveni-odborne-pracovni-skupiny-pro-hybridni-hrozby-154226/).



for example, a person's skin color, nationality, ethnicity, gender, sexual orientation or identity, religion, faith, worldview, age, disability, etc. Hate speech can be included in a broader category of hate violence, which includes not only verbal but also physical attacks motivated by hatred against certain vulnerable groups of the population.<sup>12</sup>

Hate speech on the internet can primarily be dealt with as a misdemeanor within the scope of one of the laws dealing with misdemeanors:

In this regard, it may be a misdemeanor against civil cohabitation which a person commits by causing harm to another for their affiliation with a national minority, for their ethnic origin, race, color, sex, sexual orientation, language, faith, religion, age, disability, for their political or other beliefs, membership or activity in political parties or political movements, trade unions or other associations, for their social origin, property, gender, health or marital status.<sup>13</sup>

A fine of up to CZK 20,000 can be imposed for this offense.<sup>14</sup>

If hateful behavior on social media and networks exceeds a certain threshold, it needs to be assessed by law enforcement authorities. They then assess whether the features of the substance of the crime have been met. Which criminal offenses are concerned can largely be derived from the Ombudsman's 2020 research entitled "Hate Speech on the internet" ("Nenávistné projevy na internetu"). In this material, hate crime is professionally described as a so-called tri-clinic system,

where the prejudicial motive is part of the basic factual nature of some criminal offenses, the perpetrator of these offenses is liable to imprisonment for up to three years. Furthermore, for selected crimes, prejudicial motivation appears as a circumstance that is a condition of the use of a higher mandatory sentencing, the so-called qualified factual basis. Hateful motive is then also included in the Criminal Code as a so-called general aggravating circumstance, which applies if the factual nature of a specific crime does not contain a special aggravating circumstance (qualified factual substance). A general aggravating circumstance is taken into account when deciding on the amount of the sentence, which is then imposed within the basic mandatory sentencing.<sup>15</sup>

In relation to hate speech and displays of hatred and crime, the main focus is on the most frequently committed crimes; in this respect, it is based on the analysis of the Ombudsman, prepared since 2016 and, due to its expertise, has a high

---

<sup>12</sup> A. Šabatová, "Nenávistné projevy na internetu a rozhodování českých soudů," No. 47/2019/DIS/PŽ, No.: KVOP-2720/2020 (Výzkum veřejného ochránce práv, 2020).

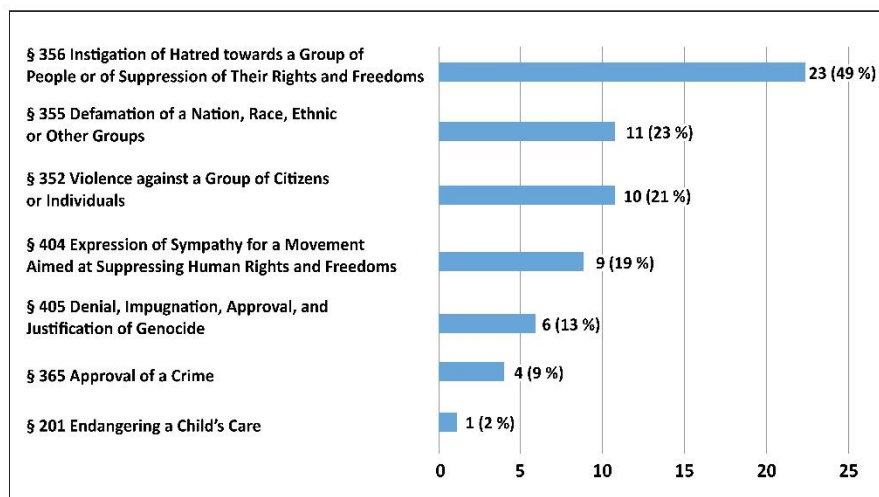
<sup>13</sup> The provisions of § 7 para. 3 let. b) of the Act on Certain Misdemeanors.

<sup>14</sup> According to § 7 para. 4 let. b) of the Act on Certain Misdemeanors.

<sup>15</sup> Ombudsman, "Nenávistné projevy na internetu a rozhodování českých soudů: Výzkum veřejného ochránce práv 2020," July 25, 2020, [https://www.ochrance.cz/fileadmin/user\\_upload/ESO/47-2019-DIS-PZ-Vyzkumna\\_zprava.pdf](https://www.ochrance.cz/fileadmin/user_upload/ESO/47-2019-DIS-PZ-Vyzkumna_zprava.pdf).

informative character usable for bodies active in criminal proceedings, working with final court decisions. Attention will be paid to the selected sphere of the most frequent crimes. This is not an absolutely exhaustive list of all crimes that might be committed in connection with hate speech on the internet.

The final part of the analysis focused on the facts of the crimes and the penalties imposed. The most common factual basis (see Figure 1) was incitement to hatred against a group of persons or restriction of their rights and freedoms (Section 356 of the Criminal Code) – this occurred in almost half of the court decisions analyzed. Roughly one-fifth contained the fact of defamation of a nation, race, ethnic or other groups (§ 355); the following items included violence against a group of inhabitants and against an individual (§ 352) or expression of sympathy for a movement aiming to suppress human rights and freedoms (§ 404). According to the Ombudsman's analysis, other facts occurred less frequently.



**Figure 1: Criminal Code's Articles Invoked in Hate Crime.**<sup>16</sup>

The following are crimes related to hate speech on the internet according to Act No. 40/2009 Coll., Criminal Code (current legislation) and the most frequently committed crimes according to the Ombudsman's analysis, based on court decisions issued in the period from 2016 to June 2019. There were a total of 47 cases involving hate speech on the internet. The following offenses have been committed through an accessible computer network against a group of people (citizens) or individuals due to their actual or perceived race, ethnic

<sup>16</sup> Šabatová, A. *Nenávistné projevy na internetu a rozhodování českých soudů*, Výzkum veřejného ochránce práv 2020, No.: 47/2019/DIS/PŽ, No.: KVOP-2720/2020, p. 23.

group, nationality, political beliefs, religion, or because they are actually or allegedly non-religious.

*§ 352 Violence Against a Group of Citizens and Against an Individual*

- Threatening a group of citizens with death, injury, or large-scale damage.

*§ 355 Defamation of a Nation, Race, Ethnic Group, or Other Group of Persons*

- Public defamation of a nation, its language, a race or ethnic group, or a group of persons.

*§ 356 Incitement to Hatred Against a Group of Persons or Restriction of Their Rights and Freedoms*

- *Public incitement to hatred* against a nation, race, ethnic group, religion, class, or another group of persons or restrictions against the rights and freedoms of their members

*§ 365 Approval of a Crime*

- *Public approval* of a crime or public praise of the perpetrator;
- Rewarding or compensating the offender or a person close to them for the punishment;
- Organizing a collection for such reward or compensation.

*§ 403 Foundation, Support, and Promotion of a Movement Aimed at Suppressing Human Rights and Freedoms*

- The nature of this crime is establishing, supporting, or promoting a movement that evidently aims to suppress human rights and freedoms or which proclaims racial, ethnic, national, religious, or class resentment or resentment against another group of persons.

Although the above-mentioned factual nature of the crime is not often mentioned in the individual statistics, it is one of the most important, as it is linked to the spread of extremist ideologies, which are closely related to hate speech in both the physical and the virtual world.

*§ 404 Expression of Sympathy for a Movement Aiming at Suppression of Human Rights and Freedoms*

- *Public expression of sympathy* for the movement referred to in Section 403.

*§ 405 Denying, Questioning, Approving, and Justifying Genocide*

- *Publicly denying, questioning, approving, or justifying* Nazi, Communist, or other genocide or Nazi, Communist, or other crimes against humanity or war crimes or crimes against peace.

The above-mentioned criminal legislation covers a large part of criminal activity in cyberspace related to hate crimes and displays of hatred committed by individuals or entire groups. Demonstrating the offender's intention to support

or promote a movement that no longer exists can be problematic. This relates to movements that have historically supported or promoted radical ideas aimed at suppressing human rights and freedoms.

The essence of the problem is that according to § 403 and § 404, it is not possible to prosecute actions that would support or promote a movement that no longer exists:

Suppose the characteristics of criminal offenses under § 403 and § 404 are to be fulfilled. In that case, the existence of such a specific movement must be proven by assessing the presented evidence, and the actions of the accused must be in some form of the objective aspect of the offenses directed towards it.<sup>17</sup>

This also applies to the sale of calendars and cups depicting Nazi symbols that are symbols of a currently non-existent movement. According to amendments to the criminal law and experience, a significant percentage of acts in which the perpetrator promotes Nazi, Communist, or other crimes against humanity, war crimes, or crimes against peace could be prosecuted under Section 405, where the law includes consideration not currently valid.

In the case of hate speech on the internet, there is a need for law enforcement agencies to gather quality evidence and its subsequent analysis because the evidence might be accompanied by symbols of extremist movements aiming to suppress human rights and freedoms.

The current arrangements are set through the resolution of the Supreme Court of the Czech Republic of June 12, 2019, No. 8 Tdo 314 / 2019-43. In the case of a symbol used by a movement aiming to suppress human rights and freedoms, the Supreme Court's resolution primarily refers to the already cited conclusions of the Criminal Division of the Supreme Court of the Czech Republic Tpjn 302/2005. It further states: "If the public prosecutor does not meet their obligation to prove the existence of such a movement already in the preparatory proceedings, then not all legal features of the crime are fulfilled."<sup>18</sup> This applies not only to the duty of the public prosecutor but also to the police authority that initiated the criminal proceedings. The criminal proceedings should commence when the police authority is convinced that it has sufficient evidence at its disposal to indicate that all the elements of the criminal offense exist.

In the opinion of the Supreme Court, it is clear that if the characteristics of criminal offenses under § 403 and § 404 of the Criminal Code are to be fulfilled, *the existence of such a specific movement must be proven on the basis of presented evidence* and the conduct of the accused in some of the forms of the objective aspect of the above-mentioned criminal offenses. Law enforcement

<sup>17</sup> "Povinnost prokázat existenci hnutí směřujícího k potlačení práv a svobod člověka – část I," *Právní prostor*, February 4, 2020, [www.pravniprostor.cz/clanky/trestni-pravo/povinnost-prokazat-existenci-hnuti-smerujiciho-k-potlaceni-prav-a-svobod-cloveka](http://www.pravniprostor.cz/clanky/trestni-pravo/povinnost-prokazat-existenci-hnuti-smerujiciho-k-potlaceni-prav-a-svobod-cloveka).

<sup>18</sup> Resolution of the Supreme Court of June 12, 2019, No. 8 Tdo 314/2019-43.

agencies involved in the criminal proceedings should follow the opinion of the Supreme Court, i.e., the fact that the file refers to another decision of the Supreme Court in another case in which the existence of the movement was found is not sufficient to prove its current existence. The existence of a particular extremist movement, whether left-wing or right-wing, must be proven by direct evidence and must also come from the perpetrator, who in turn must be shown to know the essence of the propagated movement, at least in general outline. That includes knowledge that the movement was demonstrably aimed at suppressing human rights and freedoms or spreading and promoting racial, ethnic, national, religious, or class hatred or hate against a specific group of people; willingness to support or encourage this movement by their behavior; or understanding that their actions supported or promoted such a movement.

Conversely, it cannot be ruled out that a commonly used symbol will be misused for extremist purposes and, consequently, its normal use will be difficult. An example is the regular *OK* symbol (which is a hand sign used, for example, by divers to confirm that everything is fine); in the past, this happened through hoax<sup>19</sup> campaigns, as the result of which certain media outlets started seeing this gesture as a racist one. This symbol was even added to the list of racist symbols by the American non-profit organization Anti-Defamation League (ADL). This happened in 2017 because of a hoax report on the 4chan website.<sup>20</sup> This simple hand gesture, in which the thumb and forefinger touch while the other fingers are outstretched, has been used in Great Britain since the early seventeenth century and most often signifies understanding, consent, approval, or well-being. It gained its supposedly racist symbolism through a false message that first spread on the 4chan portal and other social networks. The new and different meaning thus began to be associated with Neo-Nazi culture. All this is due to a fraud perpetrated by members of the 4chan website who falsely promoted the gesture as a symbol of hatred and claimed that the gesture represented the letters “wp” standing for “white power” (see Figure 2). Unfortunately, in the case of the “okay” gesture, the scam was so successful that the symbol became a popular trolling tactic for right-wing extremists, who often published photos on social media with this symbol. In 2019, the Australian Neo-Nazi Brenton Tarrant used the symbol in a courtroom as a sincere expression of white supremacy after being arrested for the murder of 50 people in a shooting in Christchurch, New Zealand.

<sup>19</sup> The English word ‘hoax’ means: False news, Mystification, Journalistic canard, Fraud, Startle, Fiction, Prank. “Co je to hoax?” *HO@X*, <https://www.hoax.cz/hoax/co-je-to-hoax>.

<sup>20</sup> 4chan is an American imageboard, launched on October 1, 2003, which was originally focused on discussions about manga and anime.



**Figure 2: Okay Hand Gesture, © 2020 ADL.<sup>21</sup>**

Important in assessing these newly created symbols is the context of their use. That is, the person who used them, on what occasion, and in short, if there is a possible subjective aspect. Criminal proceedings should hardly be initiated if a diver uses the above symbol. We might exaggerate and speculate what the procedure would be if the symbol is used by a diver who is demonstrably a right-wing extremist or by a right-wing extremist who has a diver's license. In cases where repressive action against these symbols is being considered, it is necessary to refrain from any speculation and artificial analysis; there is a need to act reasonably and not try to create criminal liability where there is none. In the case of excessive use of extremist symbols on social media and networks, it is necessary to require their participants to maintain a certain Internet culture and ethical behavior. The requirement may come either from groups on social networks or directly from the provider, who has the right to block and subsequently delete accounts showing an extremist and radical background.

### **The Attitude of Czech Courts to Hate Speech on the Internet**

It is clear from the cases already resolved and decided that the courts in the Czech Republic are paying attention to hate speech. Of course, everything also follows from law enforcement agencies' work in this regard. Dealing with hate speech and displays of extremism on the internet is a current priority.

An example is the case of Václav Klestil, to whom the Prague High Court upheld a three-year suspended sentence for approving on the terrorist attack on mosques in Christchurch, New Zealand, on Facebook. The court found him guilty

<sup>21</sup> Anti-Defamation League (ADL), "Okay Hand Gesture," n.d., accessed March 21, 2021, <https://www.adl.org/education/references/hate-symbols/okay-hand-gesture>.

of supporting and promoting terrorism (Section 312e of the Criminal Code). Thus, the appeal court dismissed Klestil's appeal, according to which the sentence was too severe. The prosecutor in this case even called for a five-year prison term, which means that the law enforcement authorities themselves see these crimes as a high risk to society and, hence, it is in the general interest to punish this type of crime harshly. Klestil was prosecuted and convicted for his statements on the Facebook social network, where he wrote in mid-March 2019 in a commentary under an article in *Hospodářské noviny* about the attack in which 51 people were killed in New Zealand: "Someone finally had the balls to show the way to deal with the Mohammedans. Good job." The article was posted and publicly available on the newspaper's Facebook profile. He thus committed a crime that made him liable for up to fifteen years in prison. However, the first instance courts have so far punished similar conduct with suspended sentences. The court of appeal agreed with such an approach. According to the court of appeal, similar crimes are increasing. "There can be no doubt about the danger of this behavior," said the senate president Zdeněk Sovák. However, in his opinion, the man has lived a proper and decent life so far and regrets his comment. The sentence was thus sufficient as a warning for him. At the same time, the judge drew attention to the growing opinion that the defined punishment of five to 15 years for approving terrorism in print, film, radio, television, or public computer networks did not consider similar verbal comments.<sup>22</sup>

It is clear from the above case that the public prosecutor sees a public interest in prosecuting this type of hate speech on the internet. Anyone who engages in the virtual domain, open to the public, must realize they are not communicating their views to their friends at a restaurant table but to the whole world; the supposed anonymity is a mere delusion that breaks down barriers to unethical behavior.

The case of Václav Klestil is by no means exceptional. Criminal courts imposed suspended sentences in other similar cases as well. Leoš Machálek was sentenced on June 11, 2020, by the Prague Municipal Court; Machálek commented under the video depicting the slaughter of Muslims in mosques, stating, among other things, that the shooter was a "*champion*." Machálek defended himself in court by saying that he thought the video captured Allied forces' attack on radical Islamists. Machálek shared his post on the *drsnysvet.cz* server on the morning of March 17, two days after the New Zealand attack. He responded to an article entitled "This Is How the Attacker Wiped Out the New Zealand Mosque." Specifically, he wrote: "Does it sound bad that I would join that? What did that Muslim scum do to Europe? And they are being treated like lambs. They do not keep the laws of the country that welcomed them. In my opinion, he is a champion."<sup>23</sup>

<sup>22</sup> "Odvolací soud potvrdil další podmínku za schvalování vraždy 51 lidí na Facebooku. Václav Klestil dostal tři roky," *Romea.cz*, August 19, 2020, accessed August 30, 2020, <http://www.romea.cz/cz/zpravodajstvi/domaci/odvolaci-soud-potvrdil-dalsi-podminku-za-schvalovani-vrazdy-51-lidi-na-facebooku.vaclav-klestil-dostal-tri-roky>.

<sup>23</sup> "Odvolací soud potvrdil další podmínku za schvalování vraždy 51 lidí na Facebooku."

On July 8, 2020, Jiří Kantor also received the strictest possible suspended sentence. Kantor shared an article about the shooting on his Facebook profile and commented on it: “As far as I can say, a job well done.” The person of the perpetrator himself is also significant in this case. As the investigation revealed, he was highly likely to be inclined to right-wing extremism, as he had, among other things, “ACAB” and “All cops are bastards” gothic-type tattoos on his body. We only mention this to illustrate the case because Kantor defended himself by stating, among other things, that after reading the article, he thought it was good that the New Zealand police arrested the shooter so quickly and therefore wrote a comment about a well-done job. He meant the work of the police, and he never thought of possibly praising the shooter. However, this claim is refuted by the tattoos on his body.<sup>24</sup>

Renata Pelikánová also received two-year probation for her hate speech on Facebook. She wrote the following about the shooter in mosques: “Now that is a whizz. I wish that more of us were like him when the governments do nothing about the Muslim swine and even give in to them.” As a part of her post, she reportedly added that she thanked the man for his courage. Pelikánová responded to a post from the Hoj.cz server, which, according to the plaintiff, was followed on Facebook by over 160,000 people. In his opinion, she thus committed the crime of supporting and promoting terrorism, for which she was liable up to fifteen years in prison. Prosecutor Bílý acknowledged that the woman had not been sentenced before and had lived a proper and orderly life; however, due to the mandatory sentencing, he suggested that she be given an unconditional sentence.<sup>25</sup>

The cases mentioned above eloquently present the current status of social media and networks, where people act thoughtlessly and often inappropriately comment on news articles. Some do so without any ideology. The extremist background of others can be inferred. Indications that a person behaving inappropriately belongs to an extremist group may be an aggravating circumstance, but criminal proceedings as such cannot be based on these indications. In these cases, the subjective aspect of the crime must be clearly stated. This relates not only to its obligatory sign but also, optionally, the motive (reason) and the goal (intention) of the offender. For those extremist crimes where an optional feature is not required, the feature should be considered an aggravating circumstance. However, from the point of view of criminal law, we must also realize that crim-

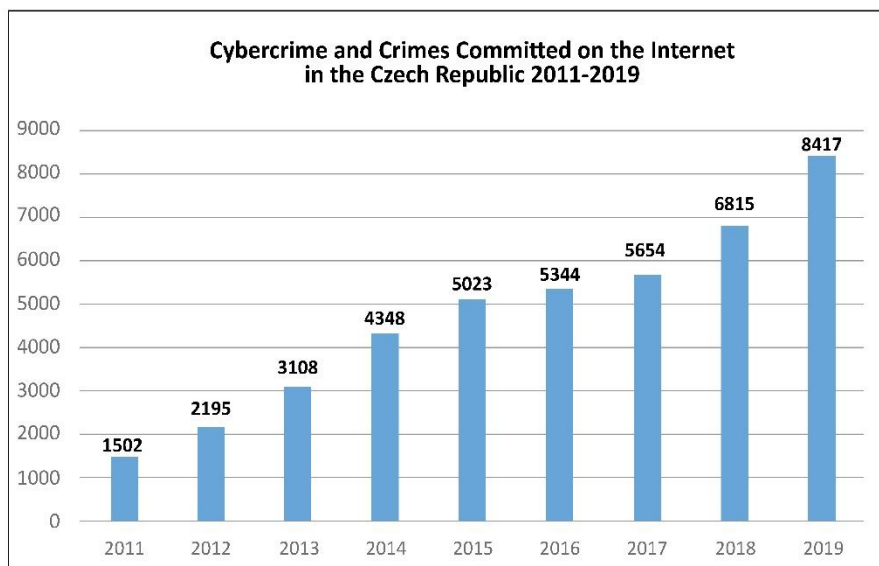
<sup>24</sup> “Za schvalování útoku v Christchurchi dostal Kantor pětiletou podmínku. Hrozilo mu až 15 let,” *iROZHLAS – spolehlivé a rychlé zprávy*, July 8, 2020, accessed August 30, 2020, [https://www.irozhlas.cz/zpravy-domov/christchurch-mesita-schvalovani-facebook-kantor\\_2007081017\\_pj](https://www.irozhlas.cz/zpravy-domov/christchurch-mesita-schvalovani-facebook-kantor_2007081017_pj).

<sup>25</sup> “Za schvalování útoku na mešity dostala žena podmínku. Žalobce pro ni žádá vězení,” *Aktuálně.cz*, June 1, 2020, accessed August 30, 2020, <https://zpravy.aktualne.cz/domaci/za-schvalovani-terorismu-dostala-zena-podminku/r~012fa30aa3e211eaa7deac1f6b220ee8/>.



inal liability cannot be built on mere presumptions and artificially created analyses or constructions. Demonstrating the offender's motive and purpose must be based on proven and substantiated evidence.

In the context of the current COVID 19 pandemic, we can expect a more significant increase in cybercrime. Statistics from 2020 are not yet available, but a look at statistics from previous years demonstrates a rapid growth of cybercrime on the internet (see Figure 3).<sup>26</sup>



**Figure 3: Cybercrime Cases in the Czech Republic, 2011-2019.** © 2020 Policie ČR <sup>27</sup>

In the coming years, we can expect a further increase in the spread of disinformation campaigns and hate speech from other political directions, and it may not always be just a clash between the ultra-left and the far-right. Social networks and media provide a platform for the clash of political campaigns and hybrid activities initiated by foreign powers, which are supposed to influence society's opinion on a particular political topic. An example is the political dispute over removing the monument to Marshal Konev in Prague 6 in 2020. The dispute over the removal turned into a political disagreement over the relations with Putin's Russia, which can be considered negative in the Czech society. However, the gates of history were opened again, and the society began to realize that it

<sup>26</sup> "Kyberkriminalita."

<sup>27</sup> "Kyberkriminalita," Policie České republiky, accessed September 17, 2020, <https://www.policie.cz/clanek/kyberkriminalita.aspx>.

still had not come to terms with the past and demanded the removal of the monument due to the criticism of the former Soviet Union and its policies. However, this situation was abused by Russia during the debate on the abolition of the monument. The case was used to revive Russian propaganda in the Czech lands. Russia is able to seize every opportunity in its disinformation campaigns, and just an insignificant event as the removal of the monument provided the ideal opportunity. The case provoked such a response in the international arena that even Russian Foreign Minister Sergei Lavrov called on representatives of Czech diplomacy to engage in dialogue on the subject, as Russia saw this as a gross violation of the 1993 agreement on friendly relations. The Czech Ministry of Foreign Affairs stated that removing the statue of Konev from the square in Prague 6 does not violate any of the Czech-Russian treaties. The statue was finally removed on April 3, 2020. This is a perfect example of how Russia can use insignificant events to its advantage and provoke international tension.

## Conclusion

If we take a critical look at the statistics published by the Police of the Czech Republic (Figure 3), we will find that crime in cyberspace is growing very quickly and that this trend will be maintained in the future. This may be due to the fact that the “virtual space” has become an integral part of our lives in which we spend our free time, educate ourselves, and even try to relax; it represents another space that allows for our self-expression. Therefore, it is important to realize that many socially unhelpful activities can occur in the cyberworld. It is already clear to society that many of the crimes can be fulfilled in cyberspace. The current legislation in the Czech Republic is sufficient to deal with hate speech on the internet. There is a need to use available legislation and quality analysis to combat this phenomenon. It will always depend on the quality of the work of law enforcement agencies. Emphasis must be placed on both operational work and investigations, presenting the police work in front of the court. Well-secured and well-established evidence is fundamental to success in court proceedings.

Through the lenses of law enforcement, cyberspace can be seen as a new domain where various types of crime are committed – from less serious ones such as fraud and theft of bank information to the most serious ones such as terrorism or attacks on critical information infrastructure of the state. The current legislation may be sufficient to prosecute hate speech and other serious crimes on the internet. Yet, it is imperative to continue developing new strategies and work on new international agreements that will make it possible to protect the principles of democracy in the virtual world. The cornerstone in this respect can be the Convention on Cybercrime,<sup>28</sup> also known as the Budapest Convention on Cybercrime, which is the first international treaty striving to harmo-

---

<sup>28</sup> 104/2013 Sb. m. s Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě.

nize national legislation in the fight against cybercrime. The Czech Republic ratified this convention in 2013. Its strength is that 68 states have already signed to date, of which 65 have ratified it; these include, for example, the USA, Canada, and most member states of the European Union, including the Czech Republic. It is necessary to continue this effort and build a strong society that will continue to carry the idea of democracy, the legacy of which was left to us by the first president of the Czechoslovak Republic, Tomáš Garigue Masaryk.

The future can be in educating the young generation, which needs to be acquainted with the pros and cons of the virtual world. Like in traffic, where it is forbidden to cross the road at a red light, the basics of ethics and decency must also apply in cyberspace, and because some people do not follow social conventions and rules, the basics must also be enforceable by the justice and law enforcement system.

## **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **Acknowledgment**

Article supported by Ministry of the Interior of the Czech Republic, project No. VI20192022117, Detection of Radicalization in the context of population and soft targets protection from violent incidents.”

## **About the Author**

**Lukáš Vilím** – see the CV on p. 20 of this issue, <https://doi.org/10.11610/Connections.20.2.02>





Holovkin, Tavolzhanskyi, and Lysodyed

*Connections QJ* 20, no. 2 (2021): 75-87

<https://doi.org/10.11610/Connections.20.2.07>

Research Article

## Corruption as a Cybersecurity Threat in the New World Order

**Bohdan M. Holovkin, Oleksii V. Tavolzhanskyi,  
and Oleksandr V. Lysodyed**

*Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi  
National Law University, <https://nlu.edu.ua/>*

**Abstract:** The important topic of cybersecurity relative to the fight against corruption in the context of global challenges in the pandemic and post-pandemic world requires further research. The purpose of this article is to identify and analyze current and prospective cybersecurity issues in this context by applying general-scientific and special-legal methods of cognition. Using the dialectical method, theoretical background, and contemporary views on ensuring cybersecurity served to investigate the key current challenges. Formal-legal and comparative methods allowed to recommend measures to enhance cybersecurity in view of the massive digitalization and social transformations. The authors emphasize the need to establish a national cybersecurity policy based on society's information literacy and culture, combining respect to traditional and historical values with a modern understanding of multicultural communication and well-being.

**Keywords:** cybersecurity, corruption, fight against corruption, cybersecurity threats, COVID-19 pandemic, post-pandemic conditions.

### Introduction

Historically, ensuring security depended on the state's power and economic and military potential. Today's state has to add one more component to the list of

obligations – to protect the digitalized parts of the state and societal activities.<sup>1</sup> Ensuring cybersecurity is one of the obligatory functions of modern countries to support and improve the system of holistic protection of society by the state. In conditions of widespread corruption, the focus shifts from the defense of rights and freedoms to some monetary profit or other benefits.<sup>2</sup> Thus, in conditions of corruption, it is hardly possible to ensure any type of security. On the one hand, corruption is already conceptually determined and perceived as a danger for every country. On the other, in the processes of globalization, digitalization, rapid technological development and innovation, and the pandemic, corruption is still an attribute of modern states, social dialogue, and communication.<sup>3</sup> The state of cybersecurity in a particular country depends on this phenomenon that is negative by its nature and destructive to the stable functioning of public authorities, expected to adequately perform their functions and earn the trust of the people.<sup>4</sup>

The traditional tools available to law enforcement agencies can no longer effectively counter corruption. Recently, the interest shifted to the value of a new institutional anti-corruption approach with a lesser role of punitive and repressive mechanisms.<sup>5</sup>

Each legal framework has its own aims and purposes and establishes its mechanisms to achieve them.<sup>6</sup> The reduction of corruption is considered one of the most important steps to pave the way for sustainable development and to promote inclusive societies by building effective, accountable, and inclusive institutions at all levels.<sup>7</sup> Practically speaking, the global anti-corruption effort does

<sup>1</sup> Mykola O. Ovcharenko et al., "Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method," *Journal of Advanced Research in Law and Economics* 11, no. 4 (2020): 1296-1304, [https://doi.org/10.14505/jarle.v11.4\(50\).26](https://doi.org/10.14505/jarle.v11.4(50).26).

<sup>2</sup> Victoria V. Tsytko et al., "Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction," *Journal of Advanced Research in Law and Economics* 10, no. 6 (2019): 1664-1672.

<sup>3</sup> Viacheslav V. Vapniarchuk et al., "Protection of Ownership Right in the Court: The Essence and Particularities," *Asia Life Science* 21, no. 2 (2019): 863-879, <http://dspace.nlu.edu.ua/handle/123456789/18141>.

<sup>4</sup> Yu. Tavolzhanska et al., "Severe Pain and Suffering as Effects of Torture: Detection in Medical and Legal Practice," *Georgian Medical News* 10 (307) (October 2020): 185-193, [http://ir.librarynmu.com/bitstream/123456789/2160/1/GMN\\_62-68.pdf](http://ir.librarynmu.com/bitstream/123456789/2160/1/GMN_62-68.pdf).

<sup>5</sup> Sergey Vorontsov et al., "The Use of Artificial Intelligence to Combat Corruption," *Media Education (Mediaobrazovanie)* 60, no. 4 (2020): 757-763, <https://doi.org/10.13187/me.2020.4.757>.

<sup>6</sup> Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation," *Computer Law and Security Review* 35, no. 6 (November 2019): 1-11, <https://doi.org/10.1016/j.clsr.2019.06.007>.

<sup>7</sup> Giulia Mugellini and Jean-Patrick Villeneuve, "Monitoring the Risk of Corruption at International Level: The Case of the United Nations Sustainable Development Goals," *European Journal of Risk Regulation* 10 (March 2019): 201-207, <https://doi.org/10.1017/err.2019.16>.

not need new rules but, rather, better implementation. The human rights approach can contribute to closing the implementation gap. The full recognition that corruption undermines the exercise of human rights allows the universal, non-adversarial human rights monitoring bodies to address corruption in detail without overstepping their mandate. By contributing to a change of the frame of reference and opening up new options for monitoring and litigation, the human rights perspective can usefully complement the criminal law approach to corruption and thereby contribute to the fulfillment of the development goals of Agenda 2030.<sup>8</sup>

Thus, the purpose of this article is to determine current issues and prospects of ensuring cybersecurity in the pandemic and post-pandemic world order under the continuous fight against corruption. Towards this aim, it is necessary to perform the following tasks:

- 1) to consider the theoretical-legal fundamentals of corruption as a cybersecurity threat;
- 2) to analyze the current state, issues, and challenges for cybersecurity in modern conditions of the fight against corruption;
- 3) to investigate particularities and suggest prospects of ensuring cybersecurity under the fight against corruption in pandemic and post-pandemic reality,

while taking into account the legally regulated relations and activity in the sphere of cybersecurity and the fight against corruption.<sup>9</sup>

General-scientific and special-legal methods of cognition have been applied towards this purpose. The subject has been investigated and the modern challenges outlined by using the dialectical method, theoretical background, and analysis of current issues. The formal-dogmatic method contributed to the development of the author's explanation of corruption as a threat to cybersecurity. Formal-legal and comparative methods provided the opportunity to formulate recommendations on enhancing cybersecurity.

## **Juridical Fundamentals of Corruption as a Cybersecurity Threat**

The provision of cybersecurity needs to be studied with the account of corruption as a threat in globalization and increasing digitalization processes. To pro-

---

<sup>8</sup> Anne Peters, "Corruption as a Violation of International Human Rights," *European Journal of International Law* 29, no. 4 (November 2018): 1251-1287, <https://doi.org/10.1093/ejil/chy070>.

<sup>9</sup> O.E. Kostyuchenko et al., "Robotization of Manufacturing Process: Economic and Social Problems and Legal Ways of Their Solution," *Financial and Credit Activity: Problems of Theory and Practice* 3, no. 30 (2019): 454-462, <https://doi.org/10.18371/fcaptp.v3i30.179847>.

vide the increasingly effective and progressive functioning of cybersecurity under the fight against corruption in conditions of pandemic and post-pandemic global order, Cherniavskiy and co-authors have made some recommendations.<sup>10</sup>

Cybersecurity as a domain of state security is based on the same range of requirements used by advanced countries in relation to the functioning and development of their security systems. At the same time, cybersecurity has a specific environment for its existence and development because a cyberattack focuses on the digital capacity of a state. Cyberattack consequences are dangerous for devices, network systems, data, and software and can destroy a state not just digitally but even physically. Among the variety of cyber threats, corruption plays one of the lead roles. It may make a protective system of a country vulnerable and even destroy it. Legal regulation of processes that may suffer under the corruption influence has always been a fairly significant issue. In times of pandemics, bringing increased digitalization of various services, processes, and activities, ensuring cybersecurity still includes the constant fight against corruption, hence the need for its scientific investigation as a cybersecurity threat. For example, to combat the corruption phenomenon, states, through their judicial authorities, focus on the following issues:

- 1) adopting a legal framework well-grounded to face pressures arising from corruption crimes;
- 2) strengthening the capacity to counter corruption, as well as related crimes, and thus reducing the cases of corruption;
- 3) setting up a professional body of specialists in all areas of activity, especially within the public area;
- 4) achieving efficient justice under the principles of respect to law and public dignity;
- 5) implementing efficient judicial mechanisms in criminal matters to provide criminal procedural functions.<sup>11</sup>

It has to be stressed that there is no universally accepted definition of corruption. There is a tendency to use the term “corruption” loosely as a catch-all term. There is also considerable disagreement over which specific acts constitute corruption. Today, probably the most used definition is the one adopted by the non-governmental organization Transparency International: “corruption is the

<sup>10</sup> Serhii S. Cherniavskiy et al., “International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization,” *Journal of Legal, Ethical and Regulatory Issues* 22, no. 3 (2019): 1-11, <https://www.abacademies.org/articles/international-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-8346.html>.

<sup>11</sup> Delia Magherescu, “Criminal Investigation of the Corruption Crimes: Evidence and Procedure in an Interdisciplinary Approach,” *Revista Brasileira de Direito Processual Penal* 6, no. 3 (2020): 1239-1270, <https://doi.org/10.22197/rbdpp.v6i3.394>.



abuse of entrusted power for private gain.”<sup>12</sup> The popular public-office-centered definition of corruption as “the abuse of public office for private gain” is no exception, of course.<sup>13</sup>

## **Role and Significance of Corruption as a Cybersecurity Threat**

The theoretical determination of corruption as a cybersecurity threat is based on its general understanding by the international community. The specifics are revealed by its connection to the particular environment for the realization of this negative phenomenon represented by cyberspace, the use of which should be as safe as possible. Security is a critical global concern manifested in problems such as protecting our cyber infrastructure from attacks by criminals and other nation-states; protecting our ports, airports, public transportation, and other critical national infrastructure from terrorists; protecting our wildlife and forests from poachers and smugglers; and curtailing the illegal flow of weapons, drugs, and money across international borders.<sup>14</sup>

Cross-national measures against corruption suffer from serious definitional imprecision. Since perceptions of corruption invariably differ from country to country, most cross-national studies sacrifice breadth for depth. Case studies, therefore, will always be important because they allow for a deeper and more rigorous understanding of how and why corruption works.<sup>15</sup> Corruption is a widespread phenomenon, increasingly normative behavior that can be curtailed by implementing various schedules of reinforcements, punishments, transparency, accountability, awareness, modeling, and psychological strategies to understand and combat corruption.<sup>16</sup> Corruption as a threat to cybersecurity may be understood as a potentially destructive phenomenon with the visible and invisible retrospective consequences of security vulnerabilities in cyberspace that make it impossible to provide and guarantee the prevention of cyberattacks and effective reduction of their negative consequences.

Classical states in different historical periods fought against various threats to keep the state sovereignty and territorial integrity and provide socio-eco-

---

<sup>12</sup> Julio Bacio-Terracino, “Corruption as a Violation of Human Rights” (International Council on Human Rights Policy, January 2008), 1-36, <https://ssrn.com/abstract=1107918>.

<sup>13</sup> Mark J. Farrales, “What is Corruption?: A History of Corruption Studies and the Great Definitions Debate” (June 2005), <https://ssrn.com/abstract=1739962>.

<sup>14</sup> Arunesh Sinha et al., “From Physical Security to Cybersecurity,” *Journal of Cybersecurity* 1, no. 1 (September 2015): 19-35, <https://doi.org/10.1093/cybsec/tyv007>.

<sup>15</sup> Farrales, “What is Corruption?.”

<sup>16</sup> Divyanshi Chugh, “Psychology of Corruption,” *The Learning Curve*, July 25, 2012, Lady Shri Ram College for Women Finalist, Young Psychologist 2012, National Paper Presentation Competition, Christ University, Bangalore, India, 1-11, <https://ssrn.com/abstract=2117247>.

conomic stability and prosperity. Most modern states, due to the high level of digitalization and rapid technological development, face new types of threats that are cyber by their nature. Thus, modern countries have to provide effective state policies to keep information sovereignty, stability, and further existence in a changed digital reality. As a phenomenon, corruption is dangerous for virtual reality too. Nowadays, the information state's development, except its economic and technological components, depends on the decisions of the state's power. If a country's governance includes corruption in decision-making, this fact lets us determine corruption as a threat to cybersecurity. Its role is quite significant due to the increase of the world informatization and the general change of the world's transition from traditional to digital. The stronger the corruption, the more vulnerable are the cybersecurity systems of individual countries and the world.

Internet infrastructure plays a crucial role in a number of daily activities. The pervasive nature of cyber systems ensures the far-reaching consequences of cyberattacks. Cyberattacks threaten physical, economic, social, and political security. They can disrupt, deny, and even disable the operation of critical infrastructure, including power grids, communication networks, hospitals, financial institutions, and defense and military systems.<sup>17</sup> For example, even dealing with such a form of democracy as elections, corruption may destroy it significantly. Elections are entering a new digital era with new opportunities and threats for the conduct and contestation of elections. Although many of these are not entirely new—perhaps being a continuation of older problems—there has been a qualitative leap in the nature of the challenges.<sup>18</sup>

Some countermeasures may cause public harm by undermining access to information and reducing transparency and accountability. The political outcry surrounding disinformation has, possibly disproportionately, metastasized the problem in the eyes of the public. Regulators should be cautious not to regulate too broadly, as the political debate is critical to an informed electorate and supporting democratic principles.<sup>19</sup> In a new concept not constrained by public sector and legal restrictions, corruption is seen as a deal between people for the exchange of favors over time. Only in the most appealing example, two agents,

---

<sup>17</sup> Jonathan Z Bakdash et al., "Malware in the Future? Forecasting of Analyst Detection of Cyber Events," *Journal of Cybersecurity* 4, no. 1 (2018): tyy007, <https://doi.org/10.1093/cybsec/tyy007>.

<sup>18</sup> Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 111-126, <https://doi.org/10.1089/elj.2020.0633>.

<sup>19</sup> Elizabeth F. Judge and Amir M. Korhani, "Disinformation, Digital Information Equality, and Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 240-261, <https://doi.org/10.1089/elj.2019.0566>.

one from the private sector and the other from the public sector, trade favors over time, with the public sector agent using his or her access to public funding.<sup>20</sup>

In our view, the destructive role of corruption as a cybersecurity threat may be understood only after its negative influence on the state becomes clear. The impact may make the state's cybersecurity vulnerabilities visible and a critical threat not just to the people's safety but even to the country's existence. Non-acceptance and lack of awareness of corruption as potential step-by-step destruction of the whole state is a wrong approach and one of the key features of cyberwar.

### **Currents Issues and Prospects of Cybersecurity under the Fight against Corruption**

During the pandemic, cybersecurity and its governance became of increased importance. At the same time, corruption is a traditional phenomenon that reflects on new relations with cyber components for various reasons. Traditionally, national governance and corruption challenges have been seen as:

- particularly daunting in the poorer countries, with the more prosperous world viewed as an example or as a benchmark,
- anchored within a legalistic framework and focused on the quality of formal institutions;
- a problem of the public sector; and
- divorced from global governance or security issues, regarded as separate fields.<sup>21</sup>

Governance and corruption remain controversial and misunderstood topics. But they are now given higher priority in development circles and by the corporate sector, including multinationals.<sup>22</sup> A large part of the project of combating institutional corruption consists of formulating rules and procedures that determine what is to count as corruption, not merely preventing conduct that is already known to be corrupt.<sup>23</sup> However, the "hacking" of democracies that is the substance of so much punditry and practitioner reporting in recent years has relatively little to do with the direct employment of cyber instruments to disrupt, degrade, or spy. Instead, the threat to democratic political systems emerges from the mismatch of new systems that now underpin the discourse and those

---

<sup>20</sup> Daniel Kaufmann and Pedro C. Vicente, "Legal Corruption," November 24, 2005, <https://ssrn.com/abstract=829844>.

<sup>21</sup> Daniel Kaufmann, "Corruption, Governance and Security: Challenges for the Rich Countries and the World," *SSRN Electronic Journal* (October 2004), <https://doi.org/10.2139/ssrn.605801>.

<sup>22</sup> Daniel Kaufmann, "Myths and Realities of Governance and Corruption," *SSRN Electronic Journal* (November 2005), <https://doi.org/10.2139/ssrn.829244>.

<sup>23</sup> Dennis F. Thompson, "Two Concepts of Corruption," Edmond J. Safra Working Papers, No. 16 (August 2013): 1-24, <https://ssrn.com/abstract=2304419>.

regulations and norms of behavior that must be adopted in years to come to safeguard the integrity of national polities.<sup>24</sup>

From our point of view, the corruption phenomenon is predisposed by the internal development of a society that is on the way to its own development towards the realization of its democratic choice. Corruption is always a kind of threat that can never be controlled and reduced if such a society includes it as a form of communication. The main issue of corruption for cybersecurity is located in the internal needs and interests of societies that are now more and more digital. If they follow the democratic way of their development, the main prospect is to remove corruption from their reality.

The increasing effort to constrain the pandemic shifted the attention from the constant requirement to fight corruption. But the second phenomenon is enriched in pandemic conditions, primarily due to the reduced societal control as a result of social distancing. Nowadays, traditional challenges to state security spread in the cyber area due to the increasing use of cyberspace and the involved technological possibilities. These call our attention to basic and interconnected security situations:

- any member of information and communication networks—whether international, state, or civilian—can be a potential victim of cyberattacks;
- cyberattacks can have serious national security and economic consequences and can endanger the daily life of a society;
- defense against threats is a task at the international, national, and individual user levels.<sup>25</sup>

In reality, the complexity of the target software could render the effects of an attack unpredictable by obscuring what happens when the attacker interferes with or disrupts the software systems. Second, since most computer systems are connected to other computer systems via the Internet, some attacks could spread across different systems. The complexity of each system and its connections mean that it is hard to predict the extent and speed of spread and impact. Third, corruption of computers could generate physical effects that cascade well beyond cyberspace and are themselves difficult to predict.<sup>26</sup>

The use of Artificial Intelligence (AI) for ensuring cybersecurity may be an object of corrupt manipulation, too. That is why the fight against this phenomenon is quite significant even here. Nowadays, AI is neither magic nor intelligent in the

<sup>24</sup> Christopher Whyte, "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare," *Journal of Cybersecurity* 6, no. 1 (2020): tyaa013, <https://doi.org/10.1093/cybsec/tyaa013>.

<sup>25</sup> Zsolt Szabó, "The Effects of Globalization and Cyber Security on Smart Cities," *Interdisciplinary Description of Complex Systems* 17, no. 3-A (2019): 503-510, <https://doi.org/10.7906/indec.17.3.10>.

<sup>26</sup> Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (March 2017): 7-17, <https://doi.org/10.1093/cybsec/tyw015>.

human-cognitive sense of the word. Instead, today's AI technology can produce intelligent results without intelligence by harnessing patterns, rules, and heuristic proxies that allow it to make valuable decisions in specific, narrow contexts. However, current AI technology has its limitations. Notably, it is not very good at dealing with abstractions, understanding meaning, transferring knowledge from one activity to another, and handling completely unstructured or open-ended tasks.<sup>27</sup> As a result, corruption may negatively impact even investments in security. For example, an executive skeptical of security investments may believe that unless a firm incurs a breach every year, it is wasting its IT security investment every year it does not suffer a breach. Alternatively, it may imply that a firm can expect to lose the equivalent of its IT security budget each time it suffers a data breach or security incident.<sup>28</sup>

Cybercrime costs include damage and destruction of data, forensic investigation, restoration and deletion of hacked data and systems, fraud, post-attack disruption to the normal course of business, stolen money, lost productivity, theft of personal and financial data, embezzlement, reputational harm, and theft of intellectual property.<sup>29</sup> At the same time, the most serious difficulty in maintaining the legitimate/malicious binary—and therefore constructing a stable foundation for cybersecurity itself—is not the range of technological, social, and economic pressures explicitly recognized by cybersecurity experts, but their implicit embrace of cyber-noir.<sup>30</sup> Thus, on the one hand, the use of technologies in a digital world is the present reality. On the other hand, corruption in this area is a permanent challenge that may lead to states' destruction. Thus, the global community should fight against this negative phenomenon not just in the physical domain but in the invisible cyber reality as well.

## **Prospects for Ensuring Cybersecurity under the Threat of Corruption**

Today's prospects of ensuring cybersecurity within a systematical fight against corruption depend on the economic performance of a country. The dominant position of the economic factor impacts the developments in every security field, including the cyber one. A corrupt environment that does not have society's and state interests in its essence may never guarantee either cyber or any other type

---

<sup>27</sup> Harry Surden, "Artificial Intelligence and Law: An Overview," *Georgia State University Law Review* 35, no. 4 (2019), <https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8>.

<sup>28</sup> Sasha Romanosky, "Examining the Costs and Causes of Cyber Incidents," *Journal of Cybersecurity* 2, no. 2 (December 2016), 121-135, <https://doi.org/10.1093/cybsec/tyw001>.

<sup>29</sup> Tabrez Ahmad, "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity" (April 5, 2020), <http://dx.doi.org/10.2139/ssrn.3568830>.

<sup>30</sup> James Shires, "Cyber-noir: Cybersecurity and Popular Culture," *Contemporary Security Policy* 41, no. 1 (2019): 82-107, <https://doi.org/10.1080/13523260.2019.1670006>.

of security. Corruption is still a threat to technological development and innovation. It has to be understood that it is potentially and practically dangerous not just for cyber but for state security.

The modern approach to cybersecurity has to be based on the understanding that corruption has to be under constant control. And when we discuss corruption, civil society has to control its country by all the possible means to remove the potential danger to the development and prosperity of its state. On the other hand, corruption will always be a strong factor in making citizens active participants in state governance. From this point of view, the gains of corruption, even on a rather low level, motivate the involvement of citizens in counter-corruption activities. Thus, citizens contribute to the common aim of development and well-being.

Nowadays, the approach to guaranteeing cybersecurity should be rational and practically oriented. It has to include two components – adequately educated and ideologically trained public administration, on the one hand, and members of a society with similar qualities on the other. The control of cybersecurity and the prediction of threats directly depend on the technical capacity. Cybersecurity in the fight against corruption needs to be ensured by protecting data, devices, networks, and software. The access of corrupt structures to their functioning should be limited.

Prevention of cyberattacks and elimination of their negative consequences on critical infrastructure facilities should be under constant control not only by the state but also by public organizations and individuals since corruption in this area can block access to financial and medical institutions and power plants in the wake of natural disasters and in military conflict. Advanced cybersecurity systems build on the coexistence of people, technologies, and processes preventing and protecting against cyberattacks. The creation and systematic support of a national cybersecurity strategy have to be added by the constant training of the population to know and observe cybersecurity principles and see corruption as an attribute of not just an economically weak but ideologically disorganized society.

Corruption is countered on several fronts. While laws and law enforcement are indispensable, countries serious about fighting corruption should also pay attention to reforming the role of government in the economy, particularly those areas that give officials high discretionary power. Recruiting and promoting civil servants on their merits and paying them a salary competitive to the private sector help attract high-quality civil servants with personal integrity. International pressure on corrupt countries, including criminalizing bribing foreign officials by multinational firms, is also a sound measure. But the success of any anti-corruption campaign ultimately depends on the reform of domestic institutions in currently corrupt countries.<sup>31</sup> A study of trends, drivers, and implications for the

---

<sup>31</sup> Shang-Jin Wei, "Corruption in Economic Development: Beneficial Grease, Minor Annoyance, or Major Obstacle?" (February 1999), <https://ssrn.com/abstract=604923>.

cyber security environment in Canada<sup>32</sup> delivers the following recommendations.

- 1) Design and deploy procedures and tools for ongoing monitoring, the objective of which will be to monitor the development of the digital ecosystem and survey the various actors and interactions, and assess the effects of these transformations on cyber security;
- 2) Align the regulatory regimes applicable to the various infrastructures, applications, and content with the resources and strategies implemented by a growing number of government actors and their private partners to quickly detect emerging digital risks and limit their impact on a constantly evolving ecosystem;
- 3) Initiate an in-depth consultation and reflection exercise to formulate proposals on how to restructure existing government institutions or create new ones to adapt the Canadian government's intervention and coordination abilities to new needs;
- 4) Intensify empirical research on the transformation of risks, standards, and practices associated with privacy protection in the digital ecosystem;
- 5) Accentuate coordination and knowledge-transfer initiatives of national and provincial authorities to accelerate and standardize the development of local capabilities.<sup>33</sup>

Therefore, with the need to counter corruption, progressive and efficient implementation of cybersecurity policies may be supported and improved by a society with the appropriate level of information literacy and culture in the symbiosis with deep respect to traditional and historical values of their nations within the ideology of national development and prosperity. Only a high level of deep respect and appreciation to own country, its heritage, values, and culture, and a modern understanding of multicultural communication for continuing personal and national development and well-being may create a reliable platform for cybersecurity.

Preserving cybersecurity is challenging. So, it turns out, is constructing cyber norms. Desired outcomes remain in the ether until there are norms (among other instruments) that spell out social expectations for the behavior that might achieve them. How these constructions come into being can be complicated, but neither cyberspace nor its norms are so impenetrable that actors ignore the var-

---

<sup>32</sup> Benoit Dupont, "The Cyber Security Environment to 2022: Trends, Drivers and Implications" (2012), <https://ssrn.com/abstract=2208548>.

<sup>33</sup> Dupont, "The Cyber Security Environment to 2022."

ious contexts, ingredients, and process tools involved. On the contrary, understanding the actual processes by which cyber norms form, diffuse, and evolve is likely to influence the future shape of cybersecurity.<sup>34</sup>

## Conclusions, Recommendations, and Limitations

It has been proved that the current cybersecurity system identifies corruption as its threat. A modern conceptual understanding of cybersecurity in pandemic and post-pandemic times of the fight against corruption builds on a variety of technical, economic, political, and even psychological tools and means to protect data, devices, networks, and software, reduce the risk of corruption undermining them, and provide a safe environment as a base of constructive activity.

This process includes two mandatory components represented by properly educated and ideologically trained public administration, on the one hand, and members of a society with similar qualities, on the other. The technical side of cybersecurity depends on the state's economic development and determines relevant models. At the same time, under the need to fight corruption in pandemic and the post-pandemic order, only societies with an appropriate level of information literacy and culture and deep respect to both traditional values and modern development may support and improve the progressive and efficient implementation of a national cybersecurity policy.

The materials in this article may be useful for researchers aiming to modernize the current cybersecurity system to respond to emerging challenges. However, in the research process, new questions and issues arose that are needed to be solved. Therefore, it is necessary to continue the investigation of methods and details of the effective practical implementation of a cybersecurity policy and its enhancement in the face of technological developments and corruption risks.

---

<sup>34</sup> Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity" *American Journal of International Law* 110, no. 3 (2016): 425-479, <https://doi.org/10.1017/S0002930000016894>.



## **Disclaimer**

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

## **About the Authors**

**Bohdan M. Holovkin** is a Doctor of Legal Sciences and Professor in the Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.  
<https://orcid.org/0000-0002-0333-9806>

**Oleksii V. Tavolzhanskyi** is with the Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.  
E-mail: [tavolzhanskyi8020@sci-univ.com](mailto:tavolzhanskyi8020@sci-univ.com)

**Oleksandr V. Lysodyed** is associated with the Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.





## Future Development of Quantum Computing and Its Relevance to NATO

**Rupert A. Brandmeier,<sup>1</sup> Jörn-Alexander Heye,<sup>2</sup>  
and Clemens Woywod<sup>2</sup>**

<sup>1</sup> School of Management, Kutaisi International University,  
<https://www.kiu.edu.ge>

<sup>2</sup> Think Tank JAM Systems Cyber Security Europe, <http://jamsys.eu>

**Abstract:** The first quantum computers are becoming a reality, and scientists working in various areas look forward to taking advantage of their enormous computational potential. At the same time, the high performance of quantum computers imposes serious risks for cybersecurity. We can expect an arms race between rival parties: a defensive side trying to ensure the privacy and dependability of stored and transmitted information and their adversaries. With this article, the authors aim to provide an overview of the status of quantum computer development, project the next steps, and investigate the impact future quantum systems may have on cybersecurity and military operations. We first discuss the basic aspects that differentiate quantum computing from classical computing and find that analogies between both domains are quite limited. The world of quantum computers is remarkably diverse already, and we elaborate that quantum simulators and universal quantum computers have “qubits” in common but still work in fundamentally different ways. Since security experts focus on upcoming trends in quantum computing, we take a look at the latest technologies and at the race for first reaching “quantum supremacy.” Finally, we provide a detailed analysis of the specific risks future quantum computers represent for established cryptosystems and conclude that asymmetric algorithms like the RSA protocol are particularly vulnerable. The dangers of quantum computing for cryptography are obvious, as is the high relevance of the safety of stored and transmitted data to the defense sector. However, we examine the capability spectrum of quantum

technologies and discover that breaking asymmetric encryption algorithms is just one facet, and other features like Grover's quantum algorithm may revolutionize the logistics of the armed forces. Satellite Quantum Key Distribution is another promising concept that may change the communication between military units. To NATO, quantum computing is a double-edged sword: the alliance needs to use the developments to benefit from the potential and be ready to counter the cyber threats. We derive ideas of what NATO should do in order to prepare for the quantum era.

**Keywords:** Quantum computing, quantum cybersecurity, quantum supremacy, cryptography, complexity theory, quantum resilience, quantum key distribution, NATO.

## Introduction

Already in our era of "classical computing," maintaining cybersecurity is an enormous challenge. After the 2007 cyberattacks on Estonia, in 2008, NATO adopted for the first time a "Cyber Defense Policy" and established the "Cyber Defense Management Authority" in Brussels.<sup>1</sup> NATO's 2010 "Strategic Concept" acknowledges the importance of hybrid threats, including cyberattacks, as complex risks characterized by not being confined by geographical limits.

For the financial industry, in particular, the perils of cyberspace are assuming alarming proportions. CyberSecurity Ventures and IBM report that ransomware attacks on newcomers to the field occur every 14 seconds. In 2016, 64% more cyberattacks targeted the finance sector than other sectors.<sup>2</sup> Man-in-the-middle attacks, i.e., the interception or manipulation of communications between two parties, represent a particular risk for financial but also for other sectors. Therefore, it is recommended that companies and agencies protect all access points by implementing a range of security measures.<sup>3</sup>

Since defensive technologies have improved, successful cyberattacks on corporate, government, or military networks increasingly require the resources of larger government or criminal organizations. The analysis of the sources of cyberattacks reveals that while many assaults on financial institutions are still carried out by small group threat actors attempting to extort money, exploitation activities aimed at government or military targets are primarily operations at the nation-state level.<sup>4</sup>

---

<sup>1</sup> Häily Laasme, "The Role of Estonia in Developing NATO's Cyber Strategy," Cicero Foundation Great Debate Paper No. 12/08 (The Cicero Foundation, December 2012), [https://www.cicerofoundation.org/wp-content/uploads/Laasme\\_-Estonia\\_NATO\\_Cyber\\_Strategy.pdf](https://www.cicerofoundation.org/wp-content/uploads/Laasme_-Estonia_NATO_Cyber_Strategy.pdf).

<sup>2</sup> Emma Olsson, "Report: FIs Warned to Prepare for Quantum Threats," *bobsguide*, December 6, 2019, <https://www.bobsguide.com/guide/news/2019/Dec/6/report-fis-warned-to-prepare-for-quantum-threats>.

<sup>3</sup> Olsson, "Report: FIs Warned to Prepare for Quantum Threats."

<sup>4</sup> J.R. Wilson, "Military Cyber Security: Threats and Solutions. U.S. Government and Military Are Taking a Lead Role in Protecting Sensitive Computers from Cyber Attack, and

Even advanced digital infrastructure protection may soon be insufficient because the availability of quantum computers will mean a new quality of cyberattacks. According to a group of economic heavyweights, including Microsoft and JPMorgan, a quantum computer of commercial relevance will be on the market by 2030, possibly as soon as 2024.<sup>5</sup> The worldwide market for quantum computing is predicted to be more than USD 10 billion by 2024.<sup>6</sup>

Such predictions are questioned by many experts, however. Invoking the need for many technical advancements, they estimate that it will take several decades to build quantum computers with the ability to crack presently used cryptosystems, and they do not rule out that such attempts may not be successful at all. Therefore, these experts are convinced that quantum computers posing a threat to established cryptography methods will not be available by 2030.<sup>7</sup> Nevertheless, managers of databases storing sensitive information with a need for long-term protection, such as classified government documents or long-dated root certificates, should look for alternatives to asymmetric algorithms.<sup>8</sup>

The expected upheaval of cryptosystems induced by quantum computing and the significance of cryptography for military operations suggest that NATO needs to begin preparing the relevant systems for quantum cyber attacks already now. However, cryptography is by no means the only field that quantum technologies will revolutionize, and some sectors, like long-distance communication, are also of high relevance to NATO. In this article, we will take a closer look at possible scenarios.

The remainder of this article is organized as follows: In Section II a, we discuss what sets the quantum computer apart from the classical computer. Section II b takes a look at the different types of quantum computers. Section II c examines aspects of quantum computing technology, and Section II d provides information on the term “quantum supremacy.” Section III analyses the difficulties of predicting the future of quantum computing. Section IV gives an overview of the problem-solving abilities of quantum computers. Section V takes a look at the impact of quantum computing on cybersecurity in general. Section VI studies how quantum skills are touching military issues and the results of our research are summarized in Section VII.

---

Solutions Finally Are on the Horizon,” *Military & Aerospace Electronics*, December 18, 2019, <https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network>.

<sup>5</sup> Olsson, “Report: FIs Warned to Prepare for Quantum Threats.”

<sup>6</sup> Walid Rjaibi, Sridhar Muppidi, and Mary O’Brien, “Wielding a Double-edged Sword: Preparing Cybersecurity Now for a Quantum World” (IBM Corporation, July 2018), <https://www.ibm.com/downloads/cas/5VGKQ63M>.

<sup>7</sup> Arthur Herman and Idalia Friedson, “Quantum Computing: How to Address the National Security Risk” (Washington, D.C.: Hudson Institute, 2018), <https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf>.

<sup>8</sup> John Preuß Mattsson and Erik Thormarker, “What Next in the World of Post-Quantum Cryptography?” *Ericsson Blog*, March 4, 2020, <https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms>.

## II. Science and Technology of Quantum Computing

### a. *Classical vs. Quantum Computer*

Let us first take a look at the differences between “classical” and “quantum” computers. In classical computers, “bits,” which can take the values zero or one (“binary system”), are represented by electrical signals, and data are processed in the form of a linear stream of bits. The classical bit is replaced by the “quantum bit” or “qubit” in quantum computers, and a qubit corresponds to a particle, e.g., photon or electron, not to an electrical signal. Quantum computing is of great interest because a small number of qubits already allows for the storage and processing of enormous amounts of data.

Similar to a bit, a qubit can also be found in one of two states upon measurement, e.g., spin up or spin down (in quantum mechanics, the spin of a particle is an intrinsic form of angular momentum). So what is the big difference between classical and quantum computing? In a classical computer, information is processed in a linear mode, and in an exponential mode in a quantum computer. The physical explanations for this distinction are that microscopic objects can be in “superposition” states (before observation, the spin state of an electron can be “up,” “down,” or a superposition of both) and that the collective state of a combined system of several microscopic objects can be a superposition of the individual states of these objects (“entanglement”).

“Entanglement” and “superposition” are only possible for quantum states, not for classical states. In a quantum computer, an ensemble of entangled qubits is prepared so that the coherent system is in a superposition of all combinatorial qubit configurations before measurement. Entanglement makes the programming of multi-qubit logical gates possible.<sup>9</sup> The coherence time is defined as the time quantum states can be used for technology.<sup>10</sup>

Let us consider the “knowledge” of an observer about a quantum mechanical system. There is a fundamental difference between the instants of time “before measurement” and “after measurement” because quantum mechanics is a statistical theory. Depending on the number of entangled qubits, the multitude of potential outcomes of the observation, which corresponds to the possible computation results, can be enormous. The “calculation,” i.e., the measurement, selects just a random single configuration of entangled qubit states out of the plentitude of possible test readings.

<sup>9</sup> David Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim,” *ExtremeTech*, October 29, 2019, <https://www.extremetech.com/extreme/300987-googles-quantum-supremacy-paper-tldr-edition>.

<sup>10</sup> Stuart A. Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD” (Alexandria, Virginia: Institute for Defense Analyses, June 2019), <https://www.jstor.org/stable/resrep22809>.

The randomness of the result of a single observation is due to the probabilistic nature of quantum mechanics. Quantum indeterminacy means that an undisturbed qubit can represent any value allowed by the superposition of states.<sup>11</sup> Without manipulation, the measurement results spin up and down are equally likely. However, each outcome is associated with an individual probability amplitude. Quantum computing corresponds to a manipulation of a qubit so that the chance to observe the preferred outcome, say spin up, is increased.<sup>12</sup> The trick will be to arrange the qubits so that the probability of a correct and a wrong answer is maximized and minimized, respectively. The experiment needs to be repeated until a sufficient sample size ensures the statistical significance of the mean result is reached.

Due to the entanglement of qubits, the measurement process in quantum computing can “create” information content that increases exponentially with the number of qubits. The qubit configuration selection step, which exploits the wave nature of quantum mechanical states, can be interpreted as the realization of a processor performing as many operations as there are possible qubit configurations at the same time. This feature is responsible for the predicted high efficiency of quantum computers in answering specific “quantum-adapted” mathematical questions.

Quantum processors are therefore not generally “faster” than classical processors in solving any type of computational problem, e.g., because they would perform more clock cycles per time unit, in the same way as the speed of classical processors is defined. Quantum processors can only outpace classical processors if the computational task can be cast in a form that allows for the utilization of the quantum mechanical wave properties of qubits. Suppose a system of entangled qubits can be arranged to selectively amplify the solution to a mathematical problem and cancel all qubit configurations corresponding to wrong answers via destructive phase interferences. In that case, a quantum processor can obtain a result much quicker than a classical processor because the required number of quantum operations (“measurements”) is much smaller than the number of classical floating-point operations.<sup>13</sup>

## ***b. Two Types of Quantum Computers***

In the previous section, we generally referred to the “quantum computer,” however, we need to be more precise about the terminology we are using here. In this section, we provide definitions (as far as possible) of different forms of quantum computing. When we mentioned the programming of multi-qubit logical

---

<sup>11</sup> George Johnson, *A Shortcut Through Time: The Path to the Quantum Computer* (New York: Alfred A. Knopf, 2003).

<sup>12</sup> Eric Jodoin, “Straddling the Next Frontier; Part 1: Quantum Computing Primer,” White Paper (Bethesda, Maryland: SANS Institute, 2014), <https://www.sans.org/reading-room/whitepapers/securitytrends/paper/35390>.

<sup>13</sup> Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

gates in the previous section, we implicitly described a property of the “universal quantum computer.” However, many other features are true for both the “quantum simulator” and the “universal quantum computer,” the two main classes of quantum computers.

The first type of quantum computer is the quantum simulator or quantum emulator. Quantum simulators can be viewed to some extent as analog systems designed to study specific quantum phenomena that are difficult to investigate experimentally and too complex for simulation with a classical supercomputer. Quantum simulators take advantage of the quantum mechanical properties of superposition and entanglement. They have been implemented in the form of different physical systems, e.g., as trapped-ion simulators or ultracold atom simulators.

Quantum annealing can be described as an analog version of quantum computing,<sup>14</sup> although quantum annealers can be dynamically configured (“programmed”) using software.<sup>15</sup> These quantum processors employ qubits that have minimal entanglement but allow for coherence times that are sufficiently long to complete the calculation.

Quantum annealers can be interpreted as quantum simulators using superconducting qubits to determine the ground states of Hamiltonians of spin systems by adiabatically ramping an external magnetic field from an initial to a final value. The Hamiltonian is a mathematical operator defining the energy levels of a quantum mechanical system. The term “adiabatic” implies that the external field is applied in a way so that the system eigenfunctions (the quantized stationary states of the system) change slowly and the occupation numbers of the states remain unchanged. Various profiles of an adiabatic ramp can be designed to adiabatically transform the initial to the final Hamiltonian. The ground state of this final problem Hamiltonian corresponds to the solution.<sup>16</sup> This approach takes advantage of quantum mechanical tunneling through potential barriers to investigate the topology of the energy surface.<sup>17</sup>

Quantum annealers are specifically designed to find the global minimum of a function with many local minima. This corresponds to tackling combinatorial optimization tasks like the Travelling Salesman Problem (TSP), i.e., problems distin-

---

<sup>14</sup> Arnab Das and Bikas K. Chakrabarti, “Quantum Annealing and Analog Quantum Computation,” *Reviews of Modern Physics* 80, no. 3 (2008): 1061-1081, <https://doi.org/10.1103/RevModPhys.80.1061>.

<sup>15</sup> Jack Krupansky, “What Is a Universal Quantum Computer?” *medium.com*, September 1, 2018, <https://jackkrupansky.medium.com/what-is-a-universal-quantum-computer-db183fd1f15a>.

<sup>16</sup> P. Richerme et al., “Experimental Performance of a Quantum Simulator: Optimizing Adiabatic Evolution and Identifying Many-body Ground States,” *Physical Review A* 88, no. 1 (July 2013): 12334, <https://doi.org/10.1103/PhysRevA.88.012334>.

<sup>17</sup> Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”



guished by a discrete search space. The computational mode of quantum annealers is based on quantum fluctuations and not on the manipulation (controlled, non-random entanglement) of qubits.

The first commercial quantum annealer was launched in 2011 by D-Wave Systems. A speedup by a factor of 108 on a set of hard optimization problems was reported in 2015 for the D-Wave 2X system as compared to the simulated annealing and quantum Monte Carlo methods.<sup>18</sup> In the D-wave Advantage Pegasus P16 system, released in 2020, the quantum annealing principle is used for calculations involving more than five thousand randomly entangled, superconducting qubits. This D-wave adiabatic quantum annealer can, e.g., be used for drug discovery.<sup>19</sup> The question of whether quantum annealers really yield advantages for solving certain optimization algorithms over classical computers remains open, though.<sup>20</sup>

The second type of quantum computer is the universal quantum computer. However, there is no unique definition of such a device.<sup>21</sup> According to Krupansky,<sup>22</sup> a universal quantum computer disposes of a sufficiently large number of qubits to solve nontrivial, general problems and can therefore be differentiated from special-purpose and fixed-function quantum computers, which are developed to address certain well defined computational tasks, i.e., from quantum simulators. In other words, what makes a quantum computer universal is a digital-processing layer that converts microinstructions into pulses for the manipulation of qubits, allowing them to perform as quantum logic gates.<sup>23</sup> In this way, all operations on a single qubit or pair of qubits can be carried out.

Since “digital” means “discrete value,” it should be mentioned that also attempts at continuous-variable quantum computing are underway, e.g., Xanadu’s optical computing project.<sup>24</sup>

As described by Krupansky,<sup>25</sup> universal quantum computers are classified according to four levels. A level 1, the quantum computer is a universal quantum Turing machine and cannot execute complex instruction sets. The abilities of the universal quantum computer classes increase at each level to finally reach level

---

<sup>18</sup> Hartmut Neven, “When Can Quantum Annealing Win?” *Google AI Blog*, December 8, 2015, <https://ai.googleblog.com/2015/12/when-can-quantum-annealing-win.html>.

<sup>19</sup> Nicole Hemsoth, “Glaxosmithkline Marks Quantum Progress with D-wave,” *TheNext Platform*, February 24, 2021, [www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave](http://www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave).

<sup>20</sup> Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

<sup>21</sup> Krupansky, “What Is a Universal Quantum Computer?”

<sup>22</sup> Krupansky, “What Is a Universal Quantum Computer?”

<sup>23</sup> Richard Versluis, “Here’s a Blueprint for a Practical Quantum Computer,” *IEEE Spectrum*, March 24, 2020, <https://spectrum.ieee.org/computing/hardware/heres-a-blueprint-for-a-practical-quantum-computer>.

<sup>24</sup> Krupansky, “What Is a Universal Quantum Computer?”

<sup>25</sup> Krupansky, “What Is a Universal Quantum Computer?”

4, characterized by quantum computers that significantly exceed the capacity and performance of a classical computer. A prerequisite to building a level 4 universal quantum computer is the entanglement of a large number of qubits during the entire time of computing, an extreme challenge.

### **c. Quantum Computing Technology**

Due to the possibilities, the interest of science and industry in building quantum computers is enormous, but the same is true for the fundamental and technological requirements. One main problem in realizing a quantum computer is the volatility of entanglement. For a quantum processor to work, it is necessary to keep a certain number of qubits in a superposition of states for a sufficiently long period, i.e., the coherence time. The inherent instability of quantum states leads to the tendency to rapidly dissipate a carefully arranged entanglement, a process called decoherence.

Since the decoherence of qubits is enhanced by external disturbances, a quantum computer must be isolated from the environment. Vacuum containers and very low temperatures are preferred conditions for quantum processors because they are conducive to the stability of qubit superposition and entanglement.<sup>26</sup>

A variety of concepts for the realization of qubits is presently under investigation: superconducting, ion trap, quantum dot, topological, spin-based, and flip-flop. Some are in a very early stage of development, and some are at a more advanced level. Quantum simulators using superconducting qubits are ready for the market. However, a qubit system that would allow for the construction of a universal quantum computer has yet to be discovered.

### **d. Quantum Supremacy**

An important term in the context of describing the status of quantum computing development is “quantum supremacy.” Although a quantum computer able to decipher asymmetric encryption (a so-called “quantum prime computer”) may still be science fiction, some experts believe that another important step in quantum computing may be close: quantum supremacy.<sup>27</sup> Quantum supremacy will be reached once a quantum computer can solve a problem, as artificially as it may be, that cannot be solved by a classical computer in any feasible amount of time.

---

<sup>26</sup> Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

<sup>27</sup> Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

In October 2019, a team of Google AI Quantum Group and university researchers<sup>28</sup> claimed to have reached quantum supremacy by randomly programming the 53 physical qubits of the “Sycamore” quantum processor, applying both single-qubit and two-qubit logical operations (logic gates).

Because of the instability of physical qubits, certain combinations of physical qubits are required to permit quantum error correction for the derivation of an abstract logical qubit. Quantum error correcting codes represent the information corresponding to the logical state of a single qubit in terms of the entangled state of an ensemble of physical qubits.<sup>29</sup> After quantum error correction for the Sycamore processor, the entangled physical qubits are reduced to a fraction of a single logical qubit.<sup>30</sup>

While in the programming step of a theoretical quantum processor all qubits might be collectively entangled, only adjacent qubits are entangled in the Sycamore. This restriction can, to some degree, be compensated by interchanging qubits, a time-consuming process and therefore detrimental to coherence.<sup>31</sup> Nevertheless, according to Arute and colleagues,<sup>32</sup> the numerical tasks accomplished by the Sycamore processor in ca. 200 seconds would take IBM’s “Summit” supercomputer 10 000 years. IBM immediately challenged the assertion of Arute and colleagues<sup>33</sup> by postulating that upgrading Summit with secondary storage would reduce the time for the simulation of Sycamore circuits down to 2.5 days, sufficiently short to invalidate the Sycamore supremacy statement.<sup>34</sup>

The dispute about the Sycamore quantum supremacy contention yields a foretaste of the challenges for the interpretation and the reliability assessment of quantum computing results that will be imposed by entering a phase characterized by the impossibility to verify these results with conventional supercomputers.<sup>35</sup>

It should not go unmentioned that the rationale of the term “quantum supremacy” has been questioned recently because it would imply the very unlikely

---

<sup>28</sup> Frank Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor,” *Nature* 574, no. 7779 (October 2019): 505-510, <https://doi.org/10.1038/s41586-019-1666-52019>.

<sup>29</sup> Giuliano Gadioli La Guardia, ed., *Quantum Error Correction. Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*, Quantum Science and Technology Series (Springer, 2020).

<sup>30</sup> Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

<sup>31</sup> Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim.”

<sup>32</sup> Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

<sup>33</sup> Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

<sup>34</sup> Edwin Pednault et al., “Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits,” *arXiv*, 2019, <https://arxiv.org/abs/1910.09534>.

<sup>35</sup> “Google’s Search for Quantum Supremacy,” *ID Quantique*, March 20, 2018, <https://www.idquantique.com/googles-search-for-quantum-supremacy>.

scenario that quantum computers might be able to generally outperform classical computers. Instead, future quantum computers are expected to be more efficient than classical computers only at solving specific tasks. Therefore phrases like “quantum advantage” and “quantum practicality” have been suggested to describe the progress in quantum computing.<sup>36</sup>

### III. Predicting the Development of Quantum Computing

It is very difficult to forecast the speed of progress in quantum computing. One reason for this uncertainty is the multitude of qubit technologies presently under consideration. In order to decide which qubit architectures will be successful in the long run, many open issues still need to be addressed, both from a theoretical and practical perspective. Another factor is the question of which impact the availability of early generation quantum computers will have on the design of subsequent generations. Finally, it is not easy to figure out on which scale other upcoming innovations like artificial intelligence may also influence the evolution of quantum computers.<sup>37</sup>

In fact, a mutual enhancement of both scientific disciplines is not unlikely since quantum computing will also have an impact on the field of artificial intelligence by performing certain operations much faster than classical computers. This anticipation stimulated the foundation of the interdisciplinary field “Quantum Artificial Intelligence” (QAI). Machine learning is a sub-field of artificial intelligence, and one discipline of QAI is consequently quantum-enhanced machine learning.

A comprehensive study of the potential impact of quantum technologies on political and military interests has been performed by the Institute for Defense Analyses (IDA) for the US Department of Defense in 2019.<sup>38</sup> According to Wolf and colleagues,<sup>39</sup> the development of digital quantum computing will follow three steps: component quantum computation (CQC), noisy intermediate-scale quantum (NISQ) computing, and fault-tolerant quantum computing (FTQC). For superconducting and trapped ions qubits, the NISQ stage has just been reached. Alternative architectures, like quantum dots, are still in the CQC realm. No qubit technology is presently close to the FTQC regime.

---

<sup>36</sup> Scott Fulton III, “What Happened to Quantum Supremacy? Quantum Computing Needs a New Success Metric,” *ZDNet*, November 2, 2020, <https://www.zdnet.com/article/what-happened-to-quantum-supremacy-quantum-computing-needs-a-new-success-metric>.

<sup>37</sup> Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

<sup>38</sup> Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

<sup>39</sup> Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

Mathematician Peter Shor proposed a quantum computer algorithm for integer factorization in polynomial time in 1994.<sup>40</sup> For the implementation of Shor's algorithm to factor a number too large for classical supercomputers, an FTQC-level processor integrating ca. 106 physical qubits is required. According to Grumbling and Horowitz,<sup>41</sup> no serious prediction on the availability of such a quantum prime computer can presently be made, but realization will probably take at least 20 years.

It remains to be seen whether Neven's law, which states that the performance of quantum computers improves at a lightning-fast doubly exponential rate as compared to classical computers, holds up to the reality check. Neven's law can be interpreted as describing the evolution of qubit numbers in quantum processors in analogy to Moore's law predicting the number of transistors in conventional processors.<sup>42</sup>

#### IV. The Suitability of Quantum Computers for Solving Specific Problems

Quantum computers will not generally outperform classical computers in solving problems by a uniform margin. Instead, the advantage of quantum computers over classical computers will depend strongly on the nature of the task to be performed. It has been shown that quantum algorithms have the potential to massively beat classical algorithms in solving a small subset of problems. However, for the solution of many other types of problems, it appears that quantum computers will not make a big difference.<sup>43</sup> Quantum computers can have the edge over classical computers when it comes to finding the global properties of mathematical systems. Still, we will discuss in this section that also, in this case, the improvement of computational efficiency achievable with quantum algorithms depends on the particular nature of the problem.

Before continuing, we need to differentiate between the tasks of finding and of verifying solutions. For decision problems of complexity class  $P$ , solutions can be found and verified in polynomial time. Solutions to problems of class "nondeterministic polynomial time" ( $NP$ ) may not be found in polynomial time but can be verified in polynomial time. Decision problems are referred to as  $NP$ -complete

---

<sup>40</sup> Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35<sup>th</sup> Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994), 124-134.

<sup>41</sup> Emily Grumbling and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019).

<sup>42</sup> Preuß Mattsson and Thormarker, "What Next in the World of Post-Quantum Cryptography?"

<sup>43</sup> Scott Aaronson, "The Limits of Quantum Computers," *Scientific American* 298, no. 3 (March 2008): 62-69; Chad Orzel, "What Sorts of Problems Are Quantum Computers Good for?" *Forbes*, April 17, 2017, <https://www.forbes.com/sites/chadorzel/2017/04/17/what-sorts-of-problems-are-quantum-computers-good-for>.

if no polynomial-time algorithms, classical or quantum, provide solutions to them that are known.

One example of a “quantum problem” is the decomposition of an  $n$ -digit number into prime factors. The solution can obviously be verified in polynomial time. However, with the best-known algorithm for classical computers, the number of steps increases exponentially with  $n$ . Therefore, the factoring problem is believed to belong to class  $NP$  outside of  $P$ . Shor’s quantum algorithm defines the factoring task as a global property of the number and meets this challenge in polynomial time (the algorithm scales with  $n^2$ ).<sup>44</sup> Consequently, the factoring problem is not  $NP$ -complete.

However, this performance of Shor’s algorithm does not mean that quantum algorithms will always deliver exponential speedups when it comes to searching for global properties of mathematical systems. A nice example is TSP, which also relates to a global system property. In the first definition of TSP, labeled as TSP1 below, the challenge is to find a route connecting all  $n$  nodes of a network that does not exceed the given length  $L$ . If  $S$  quantifies the number of routes, then  $S$  grows exponentially with  $n$ . A classical approach will require  $S/2$  attempts on average to find a route matching the condition.

In order to classify the effort for verification of a solution to the TSP, it is important to pay attention to the specific formulation of the puzzle: if it is stated as in TSP1, then verification of the solution can obviously be performed in polynomial time. Grover’s quantum algorithm can identify a connection in ca.  $S^{1/2}$  steps, which represents a significant improvement as compared to the classical approach but does not reduce exponential scaling to polynomial scaling. This result shows that TSP1 is the same type of problem as searching an unsorted database. Although TSP1 is related to a global property of the network, so far no classical or quantum algorithm solving TSP1 in polynomial time has been discovered, and therefore, TSP1 is believed to be an  $NP$ -complete problem.

Another version of TSP is the search for the shortest connection between the  $n$  nodes (referred to as TSP2 in the following). In order to answer the question of the minimal route, it is not sufficient to check whether the length of one suggested solution satisfies the condition of undercutting a certain limit. Still, it is required to compare the lengths of all possible paths. Not even a known quantum algorithm can thus verify a solution to TSP2 in polynomial time. TSP2 is probably not  $NP$ -complete but belongs to the more comprehensive  $PSPACE$  class, which includes problems that can be solved by a classical computer disposing of a polynomial amount of memory but possibly requiring exponential time scaling.  $PSPACE$  contains the complexity classes  $P$  and  $NP$ .<sup>45</sup>

So what differentiates TSP1 from the factoring problem? Shor’s algorithm takes advantage of certain mathematical properties of composite numbers and

<sup>44</sup> Shor, “Algorithms for Quantum Computation.”

<sup>45</sup> Aaronson, “The Limits of Quantum Computers.”

their factors that can be exploited to realize constructive and destructive interference patterns on a quantum computer, leading to the synthesis of the correct answer. Wrong answers are canceled out via destructive interferences. *NP*-complete problems like TSP1 appear to not allow for the creation of such interference mechanisms.

When discussing complexity classes, one should keep in mind, though, that no proofs of the nonexistence of quantum or even of classical algorithms for the solution of *NP*-complete problems have yet been produced. Nevertheless, there is clearly an analogy in the differentiation between classes *P* and *NP* on one side and between classes *NP* and *NP*-complete on the other. It is believed that  $P \neq NP$ , because no classical algorithms that would be able to solve certain problems, like factoring, in polynomial time, are known. Similarly, it appears likely that  $NP \neq NP$ -complete since no classical or quantum algorithms have yet been discovered that would permit the completion of tasks like TSP1 in polynomial time.

## **V. Quantum Computing and Security**

In our era of classical computing, primarily two classes of encryption algorithms are employed: symmetric and asymmetric. One prominent symmetric protocol is the Advanced Encryption Standard (AES), which supports three key sizes: 128 bits, 192 bits, and 256 bits. The application field of symmetric algorithms is the protection of large amounts of data, e.g., the codification of databases.

Asymmetric encryption employs the so-called public and private keys to encrypt and decrypt data, respectively. The mathematically related keys are generated by cryptographic algorithms that produce so-called one-way functions. A well-known asymmetric approach is the Rivest, Shamir, Adleman (RSA) protocol which exploits the fact that factorization of large bi-prime numbers is too time-consuming for classical computers.<sup>46</sup> Asymmetric methods are slower than symmetric methods but do not require secure channels for exchanging keys if encrypted information is supposed to be shared between two or more parties, as is necessary with symmetric algorithms.<sup>47</sup>

Quantum computing mainly represents a security threat to asymmetric cryptosystems based on prime numbers, e.g., Shor's quantum algorithm<sup>48</sup> could be used to break RSA encryption, while symmetric protocols are not relying on prime number factorization and are considered to remain safe. A future quantum computer running Shor's algorithm and powerful enough to compromise a

---

<sup>46</sup> Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications (IJACSA)* 9, no. 3 (2018), <https://arxiv.org/pdf/1804.00200.pdf>.

<sup>47</sup> Rjaibi, Muppidi, and O'Brien, "Wielding a Double-edged Sword."

<sup>48</sup> Shor, "Algorithms for Quantum Computation."

2048-bit implementation of the RSA protocol in less than a day would not be able to decipher data protected by the AES-128 protocol.<sup>49</sup>

In 1996, computer scientist Lov Kumar Grover presented a quantum algorithm for searching unsorted databases.<sup>50</sup> The database search task corresponds to a situation in which the only way to solve the problem would be to guess the input argument of a black-box function and check the correctness of the output. The Grover method significantly reduces the average number of attempts to find a specific entry in a database with  $S$  entries ( $S$  corresponds to the size of the function's domain) to  $S^{1/2}$  as compared to  $S/2$  with classical computation.

However, the main difficulty in decrypting a symmetric standard like AES is that the size of the database  $S$  increases exponentially with the key length. This scaling property is not changed by Grover's approach. Grover's algorithm can be applied to decode data encrypted by the AES protocol by searching for a key that matches a small number of plaintext-ciphertext pairs. For example, to decrypt the AES-128 algorithm ca. 265 reversible evaluations of the block cipher need to be performed in serial mode since no efficient parallelization method appears viable and quantum computation of a function is assumed to be more time consuming than classical computation.<sup>51</sup>

The risk induced by today's extensive use of asymmetric encryption stimulated the development of the so-called "quantum-safe" or "post-quantum" cryptographic algorithms. These protocols are designed for classical computers with the purpose of protecting data against decryption attempts based on quantum computers.<sup>52</sup>

The US Government recently announced that the Commercial National Security Algorithm Suite presently used for data encryption will be replaced by quantum-safe algorithms beginning of 2024, which means that the transition will not

---

<sup>49</sup> Preuß Mattsson and Thormarker, "What Next in the World of Post-Quantum Cryptography?"

<sup>50</sup> Lov Kumar Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *STOC'96: Proceedings of the 28<sup>th</sup> Annual ACM Symposium on the Theory of Computing*, July 1996, 212-219, <https://doi.org/10.1145/237814.237866>; Mavroeidis, Vishi, Zych, and Jøsang, "The Impact of Quantum Computing on Present Cryptography."

<sup>51</sup> Preuß Mattsson and Thormarker, "What Next in the World of Post-Quantum Cryptography?"

<sup>52</sup> Preuß Mattsson and Thormarker, "What Next in the World of Post-Quantum Cryptography?"; Thomas Pöppelmann, "Efficient Implementation of Ideal Lattice-Based Cryptography," Dissertation (Bochum, Germany: Ruhr-University Bochum, Faculty of Electrical Engineering and Information Technology, June 2015), [www.seceng.ruhr-uni-bochum.de/media/attachments/files/2019/11/diss\\_thomas\\_poeppelmann.pdf](http://www.seceng.ruhr-uni-bochum.de/media/attachments/files/2019/11/diss_thomas_poeppelmann.pdf); Petros Wallden and Elham Kashefi, "Cyber Security in the Quantum Era," in *Communications of the ACM* 62, no. 4 (April 2019): 120-128, <https://doi.org/10.1145/3241037>; Anne Broadbent and Christian Schaffner, (2016): "Quantum Cryptography beyond Quantum Key Distribution," *Designs, Codes and Cryptography* 78 (2016): 351-382, <https://doi.org/10.1007/s10623-015-0157-4>.



be completed until ca. 2030.<sup>53</sup> Since the secrecy of sensitive information needs to be guaranteed for 50 or more years, the US Government obviously does not expect quantum computers able to decrypt, e.g., the RSA-3072 protocol, to become available for several decades.<sup>54</sup>

Nevertheless, advanced quantum-safe functions are currently the subject of intense research. Two public-key cryptosystems that have the potential to replace the RSA protocol are random lattice-based and ideal lattice-based cryptography. The security of these methods originates from the intractability of certain computational problems on random and ideal lattices, respectively. Lattice-based schemes have been shown to yield a large variety of cryptographic tools, some of which are of a completely new type. Included are lattice-based cryptographic algorithms that qualify as post-quantum methods.<sup>55</sup>

Another public-key method is Supersingular Isogeny Diffie-Hellmann Key Exchange (SIDH). SIDH permits the establishment of a secret key between two previously unconsenting parties over an otherwise insecure communication channel. By using, with compression, 2688-bit public keys at a 128-bit quantum security level, SIDH employs one of the smallest key sizes of all post-quantum algorithms.<sup>56</sup>

Many investigations also focus on alternatives to quantum-safe cryptography developed for classical computers. One option is Quantum Key Distribution (QKD) which may provide a route to realize unauthenticated key exchange in quantum networking. QKD enables information-theoretically secure encryption, i.e., the cryptosystem cannot be compromised even if a wannabe eavesdropper would dispose of unlimited computing power.<sup>57</sup>

In order to explain this, we briefly have to return to the concepts of quantum indeterminacy and superposition of states that apply to an undisturbed qubit. Observing a quantum particle removes the superposition and implies that the superposition collapses to a single state. This fact can be exploited to ensure the privacy of communication since eavesdropping or man-in-the-middle attacks re-

---

<sup>53</sup> Jake Tibbetts, "Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers," Technical Report LLNL-TR-790870 (Lawrence Livermore National Laboratory, September 20, 2019), <https://cgsl.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf>.

<sup>54</sup> Preuß Mattsson and Erik Thormarker, "What Next in the World of Post-Quantum Cryptography?"

<sup>55</sup> Gary Stevens, "Post Quantum Cryptography: Data Security in a Post-Quantum World," *Security Boulevard*, April 14, 2020, <https://securityboulevard.com/2020/04/post-quantum-cryptography-data-security-in-a-post-quantum-world/>; Pöppelmann, "Efficient Implementation of Ideal Lattice-Based Cryptography."

<sup>56</sup> Stevens, "Post Quantum Cryptography: Data Security in a Post-Quantum World."

<sup>57</sup> Andrew Lance, John Leiseboer, and Thomas Symul, "What Is Quantum Key Distribution (QKD)?" White Paper (Quintessence Labs, 2020), [www.quintessencelabs.com/wp-content/uploads/2020/12/What-is-Quantum-Key-Distribution-QKD-white-paper.pdf](http://www.quintessencelabs.com/wp-content/uploads/2020/12/What-is-Quantum-Key-Distribution-QKD-white-paper.pdf).

quire a measurement of the particle and consequent termination of the superposition of states. Such surveillance or manipulation attempts can therefore be noticed immediately.<sup>58</sup>

Since the principle enabling QKD is physical in nature and not mathematical, the protection of quantum networks via QKD is not threatened by quantum computers. The high cost means that QKD will only be used for the protection of highly sensitive links in the short term. A future QKD satellite network may allow for the safe global exchange and transport of keys.<sup>59</sup>

However, QKD applications in other cryptography fields beyond quantum networking do not appear very likely because new hardware would be necessary, and costs would be high. According to a white paper released by the UK government in March 2020,<sup>60</sup> significant investments in QKD research are not recommended because of this rather narrow deployment spectrum.<sup>61</sup>

In this article, we have so far concentrated on the function, development, and performance of quantum computing hardware. However, we also need to address the software aspect, particularly programs designed to run on quantum processors. Shor's and Grover's algorithms have already been mentioned, and it is clear that it will take many years until both procedures can be implemented on universal quantum computers.

However, the operations of future quantum processors can be simulated on classical computers already now, and prototype quantum devices for testing code are also available. Quantum programming languages are therefore under intense development. For an overview of the present status of this field, we refer the reader to the work of Garhwal and colleagues.<sup>62</sup>

## VI. Relevance of Quantum Computers to Military Applications

In a 2012 contribution to the Cicero Foundation's Great Debate Papers, Estonian security analyst Häly Laasme addressed the opportunities and challenges that quantum computing will mean for NATO.<sup>63</sup> He recommended that: "For NATO to be ready for the quantum era, the discussions concerning the possible technological shift and its consequences should be commenced sooner rather than later, especially considering NATO's current slow tempo in keeping up with cyber issues."

<sup>58</sup> Jodoin, "Straddling the Next Frontier."

<sup>59</sup> Lance, Leiseboer, and Symul, "What Is Quantum Key Distribution (QKD)?"

<sup>60</sup> National Cyber Security Center, UK Government, "Quantum Security Technologies," March 24, 2020, [www.ncsc.gov.uk/whitepaper/quantum-security-technologies](http://www.ncsc.gov.uk/whitepaper/quantum-security-technologies).

<sup>61</sup> Preuß Mattsson and Thormarker, "What Next in the World of Post-Quantum Cryptography?"

<sup>62</sup> Sunita Garhwal, Maryam Ghorani, and Amir Ahmad, "Quantum Programming Language: A Systematic Review of Research Topic and Top Cited Languages," *Archives of Computational Methods in Engineering* 28 (2021): 289-310, <https://link.springer.com/article/10.1007/s11831-019-09372-6>.

<sup>63</sup> Laasme, "The Role of Estonia in Developing NATO's Cyber Strategy."

Mathematical discoveries like Shor's algorithm are obviously very important for cryptography. Securing the communications between military units as well as sensitive data, e.g., information on the position of missiles stored on central servers, is a very high priority for military operations. Thus, building quantum resilience ranks at the top of the agenda of the cyber branches of any national defense organization.

A technology that can help protect military communications and that has already been shown to work in 2018 relies on quantum mechanics: satellite QKD.<sup>64</sup> Even though the UK government is seeing the potential of QKD for securing critical communications,<sup>65</sup> this technology is of great interest to intelligence services. Research is performed, particularly in China, to investigate the issue from both perspectives: using QKD to encrypt own information and finding ways to obtain information if an adversary is applying QKD encryption.<sup>66</sup> Nevertheless, the IDA study also concludes that challenges such as authentication and the availability of secure non-quantum alternatives will prevent a breakthrough of QKD for military applications in the near future.<sup>67</sup>

Apart from studying QKD with respect to the opportunities it offers for secure communications and the threats it imposes on reconnaissance, the development of post-quantum cryptographic methods is also of relevance to the armed forces in order to provide communication channels and databases that are sufficiently safe to permit military operations in the quantum era.

Although it does not appear likely that quantum algorithms will ever be able to solve NP-complete problems in polynomial time, the speedup in solving TSP1 from  $S/2$  computational steps required by classical computers down to  $S^{1/2}$  steps facilitated by Grover's quantum algorithm is significant. What effect on military operations could a future universal quantum computer with the ability to solve high-dimensional NP-complete problems with  $S^{1/2}$  scaling have? The nature of TSP1 already indicates that Grover's method may have an impact on military logistics. A quantum computer can possibly make navigation of tanks and support vehicles, warships, and aircraft a lot more efficient by optimizing routes connecting several military bases.

However, according to the IDA study, quantum optimization schemes such as Grover's algorithm are not likely to achieve a sufficiently large advantage over

---

<sup>64</sup> Wallden and Kashefi, "Cyber Security in the Quantum Era;" Sheng-Kai Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters* 120, 30501 (January 2018), <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.030501>.

<sup>65</sup> National Cyber Security Center, UK Government, "Quantum Security Technologies."

<sup>66</sup> Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, "Practical Challenges in Quantum Key Distribution," *npj Quantum Information* 2, Article number 16025 (2016), <https://doi.org/10.1038/npjqi.2016.25>.

<sup>67</sup> Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

classical heuristic approaches to play a substantial role, except for very large optimization problems.<sup>68</sup> In addition, quantum optimization using the Grover method requires FTQC and large quantum memory, which may be available only in the longer term.

Quantum annealers use a principle different from Grover's algorithm to perform combinatorial optimization tasks, and some systems have already reached the commercial stage. The quantum advantage of these devices is still questioned, though.<sup>69</sup>

The game of chess essentially simulates a 6th-century Indian battlefield, and the ability to successfully play games of strategy like chess continues to be of great interest for the elaboration of military tactics. Chess or Go are games of a similar quality as TSP2, i.e., they represent PSPACE problems beyond the NP boundaries. The question of the performance of quantum algorithms in playing strategy games leads directly to QAI. In fact, chess has been a key model object of artificial intelligence since the origins of this field. Traditional chess programs are based on expert knowledge for the derivation of search and evaluation functions. The AlphaGo Zero chess program is an implementation of the idea of reinforcement learning, which is a sub-field of machine learning, which is a sub-field of artificial intelligence.<sup>70</sup> Without relying on input from chess masters, by reinforcement learning from self-play, AlphaGo Zero demonstrated in 2018 to be a game-changer by outperforming conventional chess programs.

This progress in "classical" artificial intelligence research suggests asking whether QAI, in particular quantum-enhanced machine learning, may provide another boost to strategy game computing. Recent investigations indicate that a realization of polynomial-time solutions to strategy games through quantum algorithms will not be possible. However, substantial accelerations as compared to classical algorithms still appear feasible, similar to the TSP1 scenario.<sup>71</sup>

The IDA study further points out that one main difficulty in quantum-enhanced machine learning is the need to deal with large training datasets.<sup>72</sup> Therefore, considerable advances in designing QRAM (the quantum equivalent of dynamic random access memory, DRAM) are necessary before realizations of QAI algorithms, e.g., for playing chess, are able to compete with classical machine learning implementations like AlphaGo Zero.

---

<sup>68</sup> Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

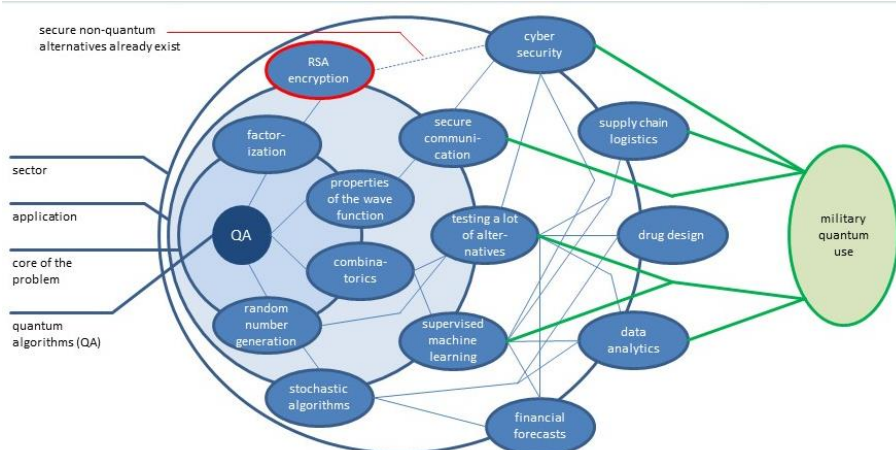
<sup>69</sup> Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

<sup>70</sup> David Silver et al., "A General Reinforcement Learning Algorithm That Masters Chess, Shogi, and Go through Self-play," *Science* 362, no. 6419 (December 2018): 1140-1144, <https://doi.org/10.1126/science.aar6404>.

<sup>71</sup> Aaronson, "The Limits of Quantum Computers."

<sup>72</sup> Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

The scheme below illustrates, in the form of a hierarchical structure, how quantum computing may affect military interests. By defining four layers, which are differentiated according to increasing complexity, three sectors (cybersecurity, supply chain logistics, data analytics) of particular relevance to the military are identified. The graphic shows how the various sectors depend on applications like supervised machine learning and how the applications themselves are connected to core disciplines of quantum computing. Drug design and financial forecasts are just two examples of civilian sectors that will be changed by quantum computing.



**Figure 1: Potential Impact of Quantum Computing on Military Interests.**

Figure 1 gives an idea of the impact quantum computing may have on selected branches of the military in graphical form. As discussed in this section, cybersecurity and supply chain logistics are sectors that are important for the armed forces and are at the same time very likely to be substantially transformed by developments in quantum computing. Data analytics is the third sector of interest to defense organizations, e.g., in the context of acquiring information on an opponent's military activities, which is also particularly susceptible to advances in quantum algorithms. Reconnaissance satellites are collecting enormous amounts of data, and quantum computers, e.g., in the context of applications of QAI, may help extract valuable information.

## VII. Summary

In Section II, we provided an overview of the scientific and technological background of quantum computer development, thus setting the basis for the dis-

cussion in the subsequent sections. Section III briefly presented prospective scenarios of quantum computing and, in particular, illustrated the difficulties complicating any predictions. Before considering specific implications of the quantum era on the military in Section VI, we first inserted a compact excursion into complexity theory (Section IV) to take a general look at the properties of quantum algorithms. Section IV's remarks exclusively refer to future universal quantum computers since they presuppose the implementation of codes like those formulated by Shor and Grover. This leads to the investigation of the impact of future quantum devices on cybersecurity in Section V.

Experts disagree on the timeframe in which a universal quantum computer with the ability to, say, break RSA-2048 encryption using Shor's algorithm will be available. This task requires the sustained entanglement of a larger number of qubits – an enormous technical challenge. Significant progress in fundamental and applied sciences will be necessary to build such a device, which involves significant uncertainty in providing a realistic perspective of quantum computing development. The US Government does not expect the commissioning of a quantum prime computer within the next several decades.

The forecasted power of such a computer to crack encryption keys is nevertheless of great interest to governmental organizations already now (cf. Section V). Quantum simulators as produced by D-Wave Systems, however, may have the ability to solve some optimization problems faster than classical computers and are already on the market. The high relevance of these quantum instruments to NATO is demonstrated by the fact that Lockheed Martin and Los Alamos National Laboratory are customers of D-Wave Systems.

The potentially high efficiency of quantum simulators in solving combinatorial optimization tasks makes them not only attractive for applications in the defense industry but also for deployments of military logistics. However, it is not yet clear whether these systems are providing a real quantum advantage.<sup>73</sup> NATO, therefore, should launch efforts to explore the risks and opportunities for its operations that are coming with quantum simulators.

The potential impact of quantum simulators on the two other sectors marked in Figure 1 as significant for the military, cybersecurity, and data analytics, is less obvious. However, these two sectors will experience massive transformations once a universal quantum computer reaches marketability.

Quantum computers able to compromise established cryptosystems may still be decades away, but NATO is nevertheless well advised to invest in the quantum resilience of its computer and network infrastructure. This can imply using full-entropy random numbers generated by quantum devices for encryption and employing longer keys for symmetric algorithms like AES. Long and fully randomized symmetric keys work for the wrapping of stored or replicated keys in order to make them quantum-safe. The crypto-agility of key managers implies their

---

<sup>73</sup> Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

compatibility with longer keys and quantum-resistant algorithms. The replacement of the RSA protocol, e.g., by quantum-safe alternatives like lattice-based cryptography or SIDH, should be given priority. Also recommended is the implementation of secure links between management nodes via QKD and/or quantum-safe algorithms. Key exchange solutions such as QKD need to be also investigated with respect to their suitability for protecting long-distance communications.<sup>74</sup>

The employment of quantum computers to support tactical operations does not appear to be a near-term option since strategy games like chess correspond to PSPACE problems beyond the NP boundaries. However, the impressive chess-playing performance of the machine-learning application AlphaGo Zero demonstrates that QAI, as a particular quantum-enhanced machine learning, may play a role for the simulation of battlefield scenarios sooner than expected by many pundits, although necessary breakthroughs like in QRAM design still represent a major obstacle for the utilization of QAI.

### **Disclaimer**

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

### **About the Authors**

**Rupert Andreas Brandmeier** studied economics (diploma) and archeology (BSc) at the Ludwig-Maximilian University (LMU), Munich. He obtained his Ph.D. degree with an analysis of the impacts of IT outsourcing. He is a Professor at the School of Management, Kutaisi International University. E-mail: [rupert.andreas.brandmeier@gmail.com](mailto:rupert.andreas.brandmeier@gmail.com)

**Jörn-Alexander Heye** is a partner of JAM Systems Cyber Security Europe OÜ, Tallinn, Estonia, with over 28 years of international experience as a director and general manager. He is a German signal officer (reserve) in national and international deployments. E-mail: [jhey@jamsys.eu](mailto:jhey@jamsys.eu)

**Clemens Woywod** is a researcher for JAM Systems Cyber Security Europe OÜ in Munich. He is also affiliated with the chemistry department at the Technical University Munich. He earned a doctorate and a habilitation degree in theoretical chemistry from TU Munich. E-mail: [clemens.woywod@ch.tum.de](mailto:clemens.woywod@ch.tum.de)

---

<sup>74</sup> "Quantum-Safe Security," *Quintessence Labs* (Canberra), 2021, <https://www.quintessencelabs.com/quantum-safe-cyber-security>.





## *Connections: The Quarterly Journal* **Submission and Style Guidelines**


*Connections* accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at [PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org) or uploaded to the journal website via <https://connections-qj.org>. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for journal future editions include:

- Arctic Exploitation and Security
- Arms Control and European Rearmament
- Challenges and Opportunities in Intelligence Sharing
- Countering and Preventing Violent Extremism
- Cybersecurity
- Defense Institution Building
- Future Security Scenarios
- Hybrid Warfare
- Limitations of Naval Power
- Migration and Refugees
- NATO's Unstable Periphery
- Putin's Russia: A Threat to Peace or a Threat to Itself?
- Terrorism and Foreign Fighters
- Trends in Organized Crime

For questions on footnotes and references, please refer to the Chicago Manual of Style, at [http://www.chicagomanualofstyle.org/tools\\_citationguide.html](http://www.chicagomanualofstyle.org/tools_citationguide.html).

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.



The Spring 2021 edition of *Connections* focuses on a number of recent challenges in the cyber domain, including the increase in cybercrime, corruption, the spread of hate speech, propaganda, and disinformation. In addition, the authors elaborate on prospective solutions such as strengthening the legal regimes, including international norms, instituting confidence-building measures, and enhancing cyber skills, as well as the challenges for defense posed by the advances in quantum computing.

For all information regarding  
CONNECTIONS, please contact:

Partnership for Peace – Consortium  
Managing Editor – LTC Ed Clark  
Gernackerstrasse 2  
82467 Garmisch-Partenkirchen, Germany  
Phone: +49 8821 750 2259  
E-Mail: [PfPCpublications2@marshallcenter.org](mailto:PfPCpublications2@marshallcenter.org)

ISSN 1812-1098  
e-ISSN 1812-2973

