Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

S.S. Costigan & T. Tagarev, *Connections QJ* 20, no. 2 (2021): 5-8
https://doi.org/10.11610/Connections.20.2.00

Editorial

Countering Crime, Hate Speech, and Disinformation in Cyberspace

Sean S. Costigan[1] *and Todor Tagarev*[2]

[1] *George C. Marshall European Center for Security Studies, https://www.marshallcenter.org/*

[2] *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[1] 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[2] and people in cyberspace or the emerging developments and likely impacts of quantum computing,[3] 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.[4] 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[5] and

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.[6] Disinformation campaigns move across borders and target individuals with precision, putting individual resiliency and critical thinking to the test.[7] 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.[8] 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.[9] 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.

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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