*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

Ш. Костиган & Т. Тагарев, *Connections QJ* 20, № 2 (2021): 5-8
https://doi.org/10.11610/Connections.rus.20.2.00

**Редакционная статья**

# Борьба с преступностью, ненавистью и дезинформацией в киберпространстве

***Шон Костиган,*[1] *Тодор Тагарев* [2]**

[1] *Европейский центр исследований в области безопасности им. Джорджа Маршалла, https://www.marshallcenter.org/*

[2] *Институт информационно-коммуникационных технологий, Болгарская академия наук, София, Болгария, http://www.iict.bas.bg/EN*

**Аннотация**: Развитие связи и открытый доступ к Интернету дают злоумышленникам новые возможности для сбора информации, атак на уязвимые цели и формирования массового сознания и поведения. В редакционной статье этого выпуска *Connections* редакторы издания анализируют новые угрозы безопасности и реакцию на них. В центре внимания – рост киберпреступности, коррупция, распространение языка ненависти, пропаганды и дезинформации. Авторы также предлагают решения – усиление правового режима, в том числе международных норм, применение мер доверия и развитие кибернавыков, а также описывают вызовы для обороны, возникающие в результате развития квантовых вычислений.

**Ключевые слова**: киберпреступность, язык ненависти, дезинформация, стойкость, коррупция, квантовые вычисления.

Сегодня киберпространству серьёзно угрожает ряд проблем в основном политического характера. Такая гуманизация киберпространства может обрадовать тех, кто годами беспокоился о слабом политическом интересе “верхов“ к единственному новому мировому «царству». Теперь, когда тема киберпространства так актуальна, легко забыть, что из-за своей условности кибернетика всегда считалась слишком технической сферой, чтобы привлечь внимание элиты – пока внезапно она не стала столь актуальной. Но по мере того, как кибернетика тихо развивалась и приобретала влияние, знающие

люди поняли, что кибернетика — не просто техническая проблема, и начали разрабатывать программы обучения и формировать новую область знаний, которая по своей природе является комплексной и междисциплинарной. Как не может быть кибернетики без технологий, точно так же не может быть кибернетики без людей.

Показательным примером служит этот выпуск *Connections*. Вниманию читателей предлагается восемь оригинальных статей о новых вызовах, выходящих за рамки организованных государствами кибероперацій[1]: это киберпреступность, коррупция, распространение языка ненависти, пропаганды и дезинформации в киберпространстве, а также решения в области технологий, политики, законодательства, образования и обучения.

Говорим ли мы о формировании доверия между частными компаниями[2] и людьми в киберпространстве или о развитии и вероятных последствиях квантовых вычислений,[3] мы вступаем в уникальную эпоху изучения кибербезопасности. Технологии будут и дальше развиваться, порождая новые проблемы, но зрелая политика и наука, примеры чего мы видим в этом выпуске, помогут увидеть эти изменения и обеспечить надёжность. Технологии и политика неразрывно связаны. Кибербезопасность – уже не просто необходимая, но в значительной степени недостаточная техническая задача, направленная на то, чтобы сделать продукты более безопасными. Это сформировавшаяся область знаний с десятками взаимосвязанных, одинаково важных областей исследований.

С ростом проблем возрастает важность людей, их знаний и навыков.[4] С каждым годом население мира всё больше зависит от киберпространства и кибербезопасности. Некоторые политические системы боятся мощи киберпространства, делая ставку на более сложные системы и сети для контроля мыслей своих граждан[5] и формирования их поведения и политической

---

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.

судьбы. Во многих странах ставят цель отделения от Интернета.[6] Кампании дезинформации пересекают границы и точечно воздействуют на людей, подвергая испытаниям их стойкость и критическое мышление.[7] Исследования этой проблемы показывают, насколько сейчас важны кибернавыки для деятельности общества.

Из-за демократизации инструментов и знаний киберпреступники сейчас могут иметь такие же возможности, как государства или большие корпорации. Многие некогда мелкие группировки выросли в преступные картели, некоторые даже предлагают совершение преступлений в качестве услуги, в то время как власть и полиция ведут борьбу с новым видом киберпреступности.[8] Государства также используют новую угрозу киберпреступности, чтобы оправдать кардинально отличные воззрения на киберпространство.

Тем временем мировые проблемы с людскими ресурсами препятствуют нашей коллективной способности защитить киберпространство и усовершенствовать инфраструктуру, которой мы пользуемся.[9] Чтобы удовлетворить эту потребность, программы кибербезопасности должны готовить специалистов, знающих все аспекты кибербезопасности: людей, процессы и технологии.

Этот выпуск *Connections* посвящён всем нашим неустанным специалистам в области кибербезопасности. Мы благодарны за ваши усилия и понимание своей миссии.

Наконец, большое спасибо – авторам издания за их терпение, позволившее наконец собрать этот интересный выпуск.

## Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнерство ради мира», организаций-участниц или издателей Консорциума.

---

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.

## Благодарность

*Connections: The Quarterly Journal*, Vol. 20, 2021, вышел при поддержке правительства США.

## Об авторах

**Шон Костиган** – профессор Европейского центра исследований в области безопасности им. Джорджа Маршалла и старший консультант рабочей группы по новым угрозам безопасности Консорциума программы «Партнерство ради мира».
*Электронная почта*: sean.costigan@marshallcenter.org

Д-р **Тодор Тагарев** – опытный политик в области безопасности и обороны с глубокими знаниями кибернетики, теории и практики управления. В настоящее время – профессор Института информационно-коммуникационных технологий Болгарской академии наук, где он возглавляет Центр управления безопасностью и обороной. Профессор Тагарев – член редколлегии *Connections: The Quarterly Journal* с 2004 года. https://orcid.org/0000-0003-4424-0201