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

Matthias Klaus, *Connections QJ* 20, no. 2 (2021): 21-31
https://doi.org/10.11610/Connections.20.2.03

Research Article

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.[1] 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

[1] 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.[2] 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.[3]

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.[4] Huawei's status as a "national champion" of a high-profile industry such as ICT[5] enabled it to become the world's largest telecom equipment and second-largest smartphone manufacturer.[6]

Huawei claims to be a private company,[7] 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.[8]

---

2 "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.

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

4 "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.

5 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.

6 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.

7 "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.

8 "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).[9] 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.[10] A risk profile from 2018 shows that Huawei also received billions of dollars in funding from several state banks in China.[11] 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.[12]

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.[13] 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-

---

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

10 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.

11 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.

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

13 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.[14] In particular, Article 7 gives cause for scrutiny. China has assured that Article 7 is misunderstood and poses no security risk.[15] In response, Huawei tasked a Chinese law firm to confirm this,[16] but critics have pointed out that legal assessments do not adequately address the concerns.[17] 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.[18] 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[19] 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[20] 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,[21] helping developing countries to overcome the barriers to technology acquisition.

---

[14] People's Republic of China, National Intelligence Law of the People's Republic, June 27, 2017.

[15] 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.

[16] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

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

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

[19] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

[20] Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

[21] 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.[22] 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.[23]

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.[24] They encompass information exchanges and cooperation between nations to combat illegal cyberattacks of various forms.[25] Due to their origin in classical arms control, international actors can also constitute CCBMs as bilateral or multilateral agreements.[26] They increase the overall feeling of security among nations by demonstrating the good intention of all participants.[27] 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-

[22] 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.

[23] 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.

[24] 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).

[25] 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.

[26] 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).

[27] Erica D. Borghard and Shawn W. Lonergan, "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.[28]

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.[29] 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.[30] 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.[31] 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,"[32] 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

[28] 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.

[29] 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.

[30] Borghard and Lonergan, "Confidence Building Measures for the Cyber Domain."

[31] 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.

[32] Hitchens and Gallagher, "Building Confidence in the Cybersphere."

compromise private sector tools and networks for their own uses."[33] 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."[34] 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.[35] 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."[36] It acknowledges that not only companies but also governments could come into a

[33] Hitchens and Gallagher, "Building Confidence in the Cybersphere."

[34] Pawlak, "Confidence-Building Measures in Cyberspace."

[35] "The Prague Proposals: The Chairman Statement on Cyber Security."

[36] "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.[37]

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.[38]

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.[39] 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.[40] 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.[41] The HCSEC aims to "demonstrate an increase in Huawei's

---

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

38 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/.

39 "Huawei's Position Paper on Cyber Security."

40 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.

41 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.

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,"[42] 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.

[42] 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.[43] 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.[44] 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.

[43] "The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks."

[44] 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.

Acknowledgment

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

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