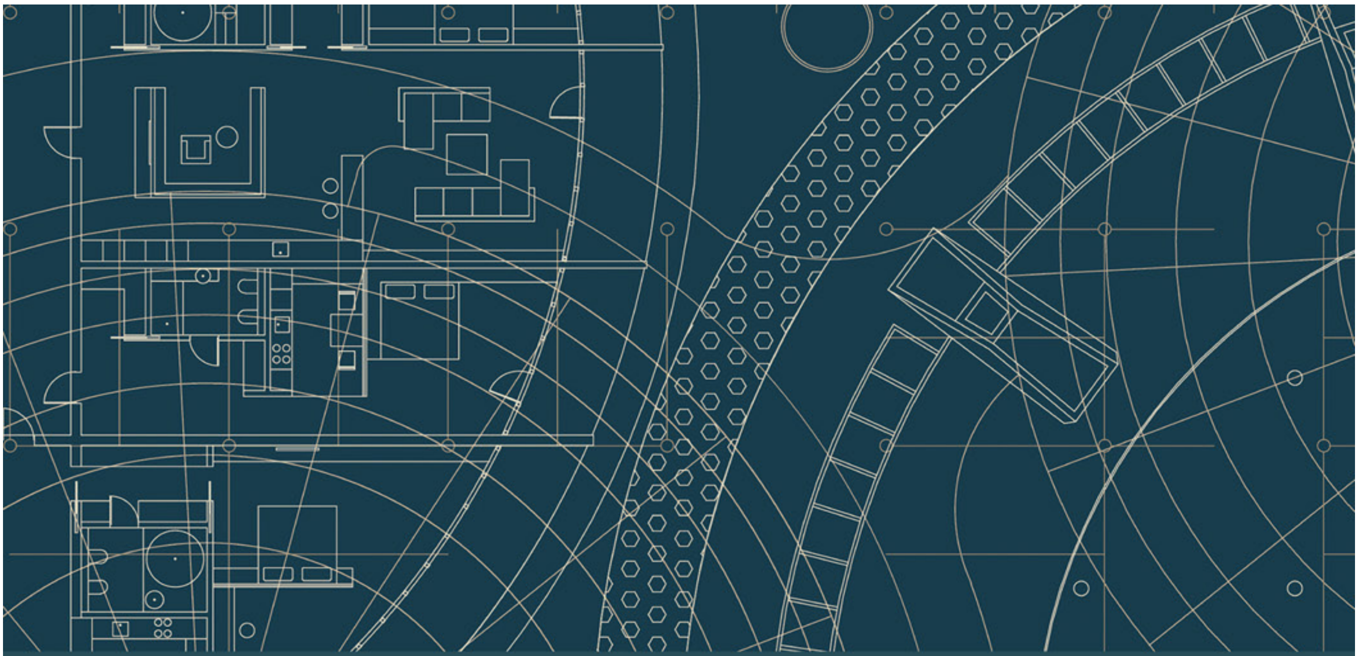

CSS Studies in Security and International Relations

CYBER SECURITY POLITICS

SOCIO-TECHNOLOGICAL TRANSFORMATIONS AND POLITICAL FRAGMENTATION

Edited by
Myriam Dunn Cavelty and Andreas Wenger

Cyber Security Politics

Socio-Technological Transformations and Political Fragmentation

Edited by Myriam Dunn Cavelty and Andreas Wenger

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2022
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging in Publication Data
Names: Dunn Cavelty, Myriam, editor. | Wenger, Andreas, editor.
Title: Cyber security politics: socio-technological transformations
and political fragmentation/edited by Myriam Dunn Cavelty and
Andreas Wenger.
Description: 1 Edition. | New York, NY: Routledge, 2022. |
Series: CSS studies in security and international relations | Includes
bibliographical references and index.
Identifiers: LCCN 2021053423 (print) | LCCN 2021053424 (ebook) |
Subjects: LCSH: Information society–Political aspects. | Computer
security–Political aspects. | Cyberspace–Political aspects. | Uncertainty.
Classification: LCC HM851 .C957 2022 (print) | LCC HM851 (ebook) |
DDC 005.8–dc23/eng/20211108
LC record available at https://lccn.loc.gov/2021053423
LC ebook record available at https://lccn.loc.gov/2021053424

ISBN: 978-0-367-62674-7 (hbk)
ISBN: 978-0-367-62664-8 (pbk)
ISBN: 978-1-003-11022-4 (ebk)

DOI: 10.4324/9781003110224

Typeset in Times New Roman
by Deanta Global Publishing Services, Chennai, India

Contents

PART I
Socio-technical transformations and cyber conflict trends 15

PART II

Illustrations

Figures

Tables

Note on Contributors

Editors

Myriam Dunn Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich. She is the author of *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge 2008).

Andreas Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS). The focus of his main research interests lies on security and strategic studies, the history of international relations, and Swiss security politics.

Authors

Farzaneh Badiei (Yale Law School) is the former executive director of Internet Governance Project at Georgia Institute of Technology. For nearly a decade, Farzaneh has been researching and directing projects related to the internet and online platforms.

Marie Baezner works at the Swiss Federal Department of Defense, Civil Protection and Sport. Earlier, she worked as a senior researcher at the Center for Security Studies at the ETH Zurich. Her main publications focused on the use of cyber means in political conflicts and on the use of military reserve forces in cyber security.

Matteo E. Bonfanti is senior researcher at the Center for Security Studies at the ETH Zurich. His research activities focus on the governance implications generated by the development and adoption of new technical, technological, and organizational solutions to enhance cyber security, policing and intelligence cooperation, as well as crisis management.

Aaron F. Brantly is an assistant professor of political science at Virginia Tech and a senior research scientist at the United States Army Cyber Institute at West Point, New York. He is the author of *The Decision to Attack: Military and Intelligence Cyber Decision-Making*.

Sean Cordey is a researcher for the Center for Security Studies at the ETH Zurich. He holds a dual degree from the Fletcher School and the University of St. Gallen. His research has notably focused on national cyber security strategies, cyber-enabled influence operations, and technologies of surveillance.

Jacqueline Eggenschwiler is a doctoral researcher at the University of Oxford. Her research looks at the contributions of non-state actors to global cyber security norm formation processes and corresponding governance implications. Jacqueline holds degrees in international affairs and governance, international management, and human rights from the University of St. Gallen and the London School of Economics and Political Science.

Johan Eriksson is professor of political science at Södertörn University, Stockholm. His research is focused on international relations, particularly the politics of technology and expertise. He is currently leading a project on post-Soviet Russian space policy. Eriksson has published seven books and numerous journal articles.

Giampiero Giacomello is associate professor of political science with the Department of Political and Social Sciences, University of Bologna, Italy, where he teaches cyber security and strategic studies. He has authored and co-edited 12 volumes and published several articles in scholarly journals.

Miguel Alberto Gomez is a senior researcher with the Center for Security Studies at the ETH in Zurich. His current research project investigates the role of cognition and affect on strategic decision-making in response to cyber security incidents. Initial findings of this project are seen in the following publications: *Sound the Alarm! Updating Beliefs and Degradative Cyber Operations* and *Past Behaviour and Future Judgements: Seizing and Freezing*.

Karl Grindal (Georgia Institute of Technology) is a doctoral student and Internet Governance Project collaborator, who previously served as the director of research for Intelligent Cyber Research (ICR), where he developed the Geocyber Risk Index (GCRI), a comparative assessment of the cyber threats.

Jasmin Haunschild is a doctoral student at the research group Science and Technology for Peace and Security (PEASEC) at the Department of Computer Science at Technische Universität Darmstadt, Germany. Her research interests include security institutions, e-government, and digitization in the public domain.

Islam Jusufi is lecturer and head of the Department of Political Sciences and International Relations at Epoka University, Tirana, Albania. His research interests relate to Balkan security politics. Most recently he published on “inclusive security and popular protests” (*Journal of Multicultural Discourses*).

Marc-André Kaufhold is a doctoral student at the research group Science and Technology for Peace and Security (PEASEC) at the Department of Computer

Science at Technische Universität Darmstadt, Germany. His research interests include crisis informatics, emergency management, information overload, and social media analytics.

Brenden Kuerbis (Georgia Institute of Technology) is a research scientist and partner in the Internet Governance Project focused on technical identifier governance and the intersection of national security concerns with forms of internet governance. Kuerbis has published in *Cyber Defense Review*, *International Studies Review*, and *Journal of Cyber Policy*, among others.

Jon R. Lindsay is an associate professor at the School of Cybersecurity and Privacy and Sam Nunn School of International Affairs at the Georgia Institute of Technology (Georgia Tech). He is the author of *Information Technology and Military Power* (Cornell 2020) and edited volumes on deterrence (Oxford 2019) and cyber security (Oxford 2015).

Amir Lupovici is a senior lecturer in the School of Political Science, Government and International Affairs and a research fellow in the Interdisciplinary Cyber Research Center, both at Tel Aviv University, Israel. His book *The Power of Deterrence* was published with Cambridge (2016).

Milton Mueller (Georgia Institute of Technology) is an internationally prominent scholar specializing in the political economy of information and communication and co-founder of the Internet Governance Project. His books include *Will the Internet Fragment?* (Polity 2017), *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010), and *Ruling the Root: Internet Governance and the Taming of Cyberspace* (MIT Press 2002).

Christian Reuter is full professor and holds the chair for Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at Technische Universität Darmstadt, Germany, with secondary appointment in the Department of History and Social Sciences.

Wolf J. Schünemann is assistant professor at Hildesheim University, Germany, with a focus on internet and politics. He has published on disinformation, cyber security, and internet governance in the *International Review of Information Ethics, New Media and Society* and the *Journal of European Integration*.

Danny Steed is a scholar practitioner and consultant, with experience across academia, government, and the private sector. Danny was a visiting fellow on the Cyber Norms Program at Leiden University, Leiden, Netherlands. His second book, *The Politics and Technology of Cyberspace*, was published with Routledge in 2019.

Stefan Steiger is a research associate at Hildesheim University and a PhD candidate at Heidelberg University, Germany. His research interests include cybersecurity policies, foreign policy analysis, and internet governance.

Christopher Whyte is an assistant professor with the program on Homeland Security and Emergency Preparedness at Virginia Commonwealth University. His research projects focus on dynamics of decision-making during cyber conflict crises, information warfare and the shape of modern cyber-enabled disinformation campaigns, and the impact of artificial intelligence on national security processes. His work is published or forthcoming with a range of scholarly journals and presses.

7 Cyberspace in space

Fragmentation, vulnerability, and uncertainty

Johan Eriksson and Giampiero Giacomello

In a novel about World War III, American leaders – confronted with the total collapse of the communication grid caused by Chinese and Russian attacks – call for help from Google and Facebook to restore communications in the United States, since these corporations have wireless infrastructure drones and blimps used in remote locations around the world (Rosone and Watson 2017). This is obviously a fictional scenario, but the fact that Google redirected its "Loon" balloons to Puerto Rico after Hurricane Maria showed that this type of action is possible, and that it was considered by US authorities. It is no longer simply fiction that cyberspace satellites are essential for the functioning of more than social media and email, but also for a vast array of critical infrastructures and societal services, through the "Internet of Things". For instance, despite the challenges to be addressed, the InterPlaNetary (IPN) has long been expected to be the next step in the design and development of deep space networks (Akyildiz et al. 2003). These increasingly space-based infrastructures will likely also be receptive targets in "information warfare" campaigns as well as in physical warfighting (Walsh and Zway 2018).

This chapter addresses the increasing interconnectedness of cyberspace and outer space, a development which opens significant questions for research as well as for strategy. While cyberspace infrastructure is increasingly dependent on space infrastructure, especially satellites, the consequences for politics and security remain uninvestigated. The chapter provides an overview of and introduction to these challenges.

Emphasis herein is on asking important questions rather than providing convincing evidence and conclusions. Further research, including both scenario-based theorizing and systematic empirical inquiry, are needed to improve both knowledge and policy. Hence, this chapter should be considered, to all intents, as a *probe*. Nonetheless, the two questions that will tentatively characterize our exploratory inquire are: (1) What are the consequences of making cyberspace increasingly reliant on satellites and other types of space infrastructure? In addition, (2) what is the meaning and significance of an interplanetary cyberspace? The latter question may seem particularly futuristic and speculative, yet the development of an interplanetary cyberspace is on the agenda within the community of technical experts (Bucur and Iacca 2017; Voosen 2016), and interplanetary

DOI: 10.4324/9781003110224-8

cyberspace is arguably an expected development given the contemporary “new space race” toward the Moon, Mars, and further into deep space.

This chapter suggests that consequences of space-based cyberspace can be analyzed in terms of three categories – fragmentation, vulnerability, and uncertainty. As will be discussed below, the development of satellite-based internet services is spearheaded by private actors, mirroring a general fragmentation and diversification of actors in both cyberspace and space. Moreover, satellite-based cyberspace implies a whole array of new vulnerabilities, as satellites can be targeted by anti-satellite missiles, and that they are vulnerable to new forms of hacking, as well as to space debris, and solar storms. More generally, these new developments are plagued with a great deal of uncertainty, in terms of how governance will be organized, what rules will apply, and whether militarization or peaceful collaboration will prevail. Uncertainty is particularly great regarding the potential development of interplanetary cyberspace, which however should not prevent discussion of what technical experts are claiming.

Cyberspace infrastructure: From Earth to space?

Cyberspace is indeed a virtual space – making real-time communication possible with little or no regard to physical distance. Simultaneously, however, cyberspace has always depended on physical infrastructure in the form of cables, routers, and servers. Moreover, it has long been known that space is a rather vulnerable environment as “[it] poses a number of challenges in providing reliable, end-to-end data communication with a tolerable level of service” (Durst et al. 1997: 389). Undersea cables have been the arteries of the internet, particularly for making global internet communications possible. Until recently, little of cyberspace communication has relied on wireless infrastructure, such as satellites and airwave (mobile communication) technology. This seems to be changing, however.

While satellite-based communication is certainly not new, it was for a long time expensive and unavailable to ordinary people, used mainly by the military, government, maritime traffic, and researchers. With the development of wireless mobile telecommunications (from the 1G to the emerging 5G and eventually 6G networks), cyberspace communication became increasingly integrated with space technology, i.e. satellites. Yet, wireless mobile telecommunications are still dependent on a grid of land-based transmission towers, which explains the prevailing dark patches of an otherwise internet-covered Earth. A complete integration of space and cyberspace has not yet taken place, but efforts are made to make cyberspace available in every part of the world.

Of interest is the “Starlink” project – initiated by multi-billionaire Elon Musk and his rocket company SpaceX. Starlink is advertised as a project to provide the entire globe with Internet access. On 29 March 2018, the US Federal Communications Commission granted SpaceX a license to set up a satellite network for the provision of broadband Internet services available across the globe (Amos 2019; Gross 2018; Choudhury 2019). Two of these satellites were launched already before the license was acquired and another 60 were launched in

May 2019. Toward the end of the 2020s, the Starlink system is expected to consist of up to 12,000 low-orbit satellites, and more will follow.

This initiative makes SpaceX a competitor to UK-based OneWeb (formerly Worldvu), which is a similar project to provide internet service to the entire globe. Other competitors are Amazon's "Project Kuiper", Google's "Project Loon", Samsung, ViaSat, Sierra Nevada Corporation, the UK-based Surrey Satellite Technology Ltd., and the Australian Gilmore Space Technologies. There are several more similar projects, of a public as well as private nature. The EU-operated Galileo satellite system is noteworthy – intended to provide services like the US Global Positioning System (GPS). Several existing and aspiring "space powers" have or are about to set up satellite-based internet services, including Russia, China, Japan, India, Brazil, and the United Arab Emirates. Consequently, the rapid rise of competitors for a satellite-based internet, a first general observation is that diversification in terms of actors involved is increasing. The wide array of entrepreneurs involved, dispersed across the Globe, suggest that fragmentation rather than hegemony will characterize this domain.

With the launch of space-based internet communications, the number of satellites orbiting Earth will increase from today's around 2,000 operative satellites to at least 20,000 satellites. Concerns have been raised that this will dramatically increase the risk of collisions, resulting in vast amounts of "space junk" (out-of-service satellites, debris from crashes, lost equipment from space walks etc.), and also interfere with transmissions, blur the vision of space telescopes, and imply dangers for space launches (Liou and Portman 2007). Undoubtedly, this development implies new vulnerabilities for space companies and their clients (including states and citizens) as well as for the space environment in itself, but also uncertainty in terms of how, when, and with what specific consequences collisions and interference occur. Vulnerability and uncertainty are also exacerbated by, on the one hand, the increasing number and diversity of space entrepreneurs and, on the other hand, the lack of national and international norms and rules adapted to this "new space race". As has often been the case, technological development moves faster than politics.

Moreover, satellite-based cyberspace might make it is easier to bypass censorship and control of access by national governments. How the information age entails a perforation of sovereignty has been suggested before, but that observation must be balanced against the legal and physical capacity of national governments to license and shut down internet service providers and take control of the physical infrastructure. With the transfer of cyber-infrastructure from Earth to space, however, there will still be a need for control centers and dishes on ground, but they can be dispersed across the globe, more easily avoiding the control of national governments. This is particularly the case when internet satellites are provided by multinational space companies, which can simultaneously operate in several countries, and which are also more mobile than any cable junctions.

Indeed, a key driver behind the development of satellite-based cyberspace is that several states have made legal changes opening of for private space projects. According to the 1968 Outer Space Treaty, states are responsible for all space activities emanating from their territories and jurisdictions (Martinez 1998). During the early Space Age, this was hardly an issue, as space was then accessible only by the governments of the United States and the Soviet Union, through NASA and its Soviet counterpart. Liberalization of space access sped up in the United States as NASA faced cutdowns and the Space Shuttle program was cancelled, and both George W. Bush Jr. and later Barack Obama argued that the private space industry must take a bigger role in space exploration, including human space exploration. The United States has spearheaded this development, which opened for companies such as SpaceX, Orbital, Boeing, Lockheed Martin, and others.

Yet other countries, traditionally not associated with space programs, have also changed their laws and opened jurisdictions for private space initiatives, and public-private partnerships. Of this a noteworthy case is Luxembourg, a small European country which over the last 10–15 years has made public-private space programs a key national strategy – specifically regarding satellites. Unlike major space powers such as the United States, Russia, China, India, and Japan – Luxembourg is not working through a national space agency with its own launch capacity but is rather opening jurisdictional space (and low taxes) for multinational space entrepreneurs, with support from the government of Luxembourg, the Planetary Resource center, and the University of Luxembourg (Araxia Abrahamian 2017).

Furthermore, the development of cyberspace in space opens the question of governance. There is clearly no overarching framework or "regime" concerning the governance of space-based cyberspace. By contrast, there is a noteworthy governance gap between the two domains. This is not surprising, however, given the fragmented governance structure regarding cyberspace and space as separate domains. For both domains, national regulation and governance dominate, as both are based on infrastructures that vary greatly between countries. In terms of global governance, the multilateral yet US-based organization ICANN maintains a key role in the governance of cyberspace, with specific authority regarding the basic technical protocols of the internet, and the internet domain name system. ICANN, together with NGOs and national governments, are also crucial in the ongoing global debate on what norms and principles cyberspace should be based upon – a debate that could be simplified as positions on "Internet freedom" and "Internet sovereignty" (Mueller 2017).

Likewise, the global governance of space is limited, with a lack of an overarching "regime" or coordinating organization (Jakhu and Pelton 2017). Yet, of fundamental importance is the Outer Space Treaty from 1967, which states that space belongs to all of humanity, that no state or private entity can claim ownership of any part of space (such as an asteroid or territory on Mars), and that weapons of mass destruction are banned from use in outer space. There are a few other global space treaties, which concern for example the Moon, liability for damages caused by space objects, the sharing of potential dangers in outer space, the use of space-related technologies, and the rescue of astronauts. These treaties are administered by the UN Office for Outer Space Affairs (UNOOSA) and the related Committee on the Peaceful Uses of Outer Space. Thus, there is a global forum for space debate and governance, yet it remains clear that authority remains largely with national governments.

As noted, while there are certain elements of global governance of cyberspace and space, these governance structures are separate. For example, it is unclear how power and authority over cyberspace in space is distributed between ICANN and UNOOSA – or other organizations, such as the International Telecommunications Union.

Moreover, it remains unclear what roles and responsibilities in global governance are held by private internet service providers and private space companies. This includes the emergence of public–private partnerships, many of which are of a transnational character (further discussed below). It is noteworthy that global space law – which is still largely state-centric – is backward in terms of the emergence of private space authority.

In sum, the development of a satellite-based internet implies a fragmentation and diversification of actors involved, the emergence of several new types of vulnerabilities (to space debris, anti-satellite missiles, etc.), and uncertainty in terms of governance (cf. Rothe and Shim 2018; Jakhu and Pelton 2017). In the following sections, we will discuss a few more specific aspects of the cyberspace-in-space development, specifically regarding security and militarization, privatization, and the potential for an interplanetary cyberspace.

Militarization of space/cyberspace?

In 2007, China shot down one of their own satellites with a ground-to-space ABM (anti-ballistic missile), which instantly removed any doubts of their anti-satellite capability. Moreover, in 2010 and again in February 2018, China used ABMs to shoot down one of their own target missiles in space (Lin and Singer 2018). Likewise, although the US "Star Wars" program of the 1980s was cancelled, in the summer of 2018 the Trump administration announced its goal of setting up a new Space Force, expanding the US military forces beyond the Army, Navy, and Air Force. It remains unknown what such a Space Force would look like, but it corroborates the general trend of militarization of space. The development of anti-satellite (ASAT) weapons precedes a potential US Space Force, and it is not limited to the United States and China. These incidents and developments can be interpreted as an indication of a more general militarization of space (Stephens 2017).

What are the implications of this development? To begin with, it means that cyberspace and internet access have become vulnerable to new forms of physical attacks. While anti-satellite weapons previously threatened certain forms of global telecommunications, they are increasingly becoming threats to the very fabrics of cyberspace. Satellite systems for telecommunications and cyberspace seem increasingly worthy of the label "critical information infrastructures" (Dunn 2006; Newlove-Eriksson et al. 2018).

The vulnerability of satellite-based cyberspace is aggravated by the development of dual-use technology, i.e. satellites which can serve both military and non-military purposes, such as a surveillance satellite that can serve the military with observations of troop movements at the same time as it serves climate research with observation of rising sea levels. The development of dual-use technology (which does not prevent the military from operating its own, single-use satellites) has been particularly strong in the United States and in Europe. A noteworthy example is the development of the EU's satellite surveillance system, which for many years bore the acronym GMES. Originally, this acronym stood for Global Monitoring for Environmental Security, which meant it was used only for civilian and scientific purposes, particularly serving climate research. In 2008, however, the EU changed the meaning of the acronym to Global Monitoring for Environment *and* Security. While this may seem as an insignificant change of language, it signaled a major policy change (Newlove-Eriksson and Eriksson 2013). Specifically, the GMES was from then and onward to be used both for civilian and military (and wider security) purposes, providing not only environmental data but also supporting the intelligence services. Later, the EU changed the name of this satellite system from GMES to Copernicus.

There is a twofold consequence of dual-use communications satellites. First, both military and civilian services are endangered if a satellite is attacked or get out of service for some other reason. Second, because of the combination of diverse types of clients – specifically military and business – there will be high demands for encryption and secrecy. Not only the risk of having satellites shot down, but also hacked into, is a new challenge. The integration of space and cyberspace means that the existing militarization of cyberspace – the world of information warfare, strategic hacking, spreading of malware and distributed denial of service attacks – become intermingled with space activities, whether civilian or military (Giacomello 2013). This may lead to an increasing difficulty in satellite-tracking and identification, as previously single-use civilian satellites by necessity are "covered up" because of their new military (and business) functions. In the long run this can be problematic as seen from the perspective of democratic accountability. In sum, the parallel militarization of space and growing dependency on space infrastructure implies great vulnerability, not only for the satellites themselves, but for the many Earth-bound infrastructures and functions they serve.

Given the great deal of uncertainty associated with space in general, it is not surprising that many stakeholders adopt a precautionary or preemptive approach. For example, the EU's approach to space security, specifically the draft International Code of Conduct for Outer Space Activities and the Space Situational Awareness program, is based on a precautionary acknowledgment of risks or threats, considering mostly preemptive measures and elements of prevention (Slann 2016). "Anticipatory security" is the norm in space and thus should be considered when assessing the transition of cyberspace from "Earth-bound" or "Earth-only" infrastructure to space.

Privatization of space/cyberspace?

The significance of private authority in the development, ownership, and operation of internet services has been acknowledged for many years. Indeed, the private sector is the "third" stakeholder in cyberspace, along with governments and users, as it is now established in the literature (Giacomello 2005, 2013: Dunn Cavelty and Suter 2009; Valeriano et al. 2018); hence as the presence of cyberspace in space grows, there will be even more incentive for the private sector to be considered *the* cardinal player. A similar growth of private authority, albeit at a slower rate, seems to be taking place with regard to space technology. As a report by the Center for Strategic and International Studies (Harrison et al. 2017: 1) noted, "commercial companies will likely be the *primary* driver of any significant reduction of the cost access to space" (emphasis added). We have yet to see complete mergers of cyberspace and space companies, and the development of new and already integrated space and cyberspace industries is still in its infancy. But, as noted above, things are changing. The expansion of SpaceX into cyberspace is a notable example.

Given the mix of government/private sector initiatives, lessons learned from past experience with public-private partnership (PPP) in critical infrastructure should be carefully considered, since, as we argued above, the private sector is likely to play the lion's part in these new fields of merging technologies (Newlove-Eriksson et al. 2018). During the privatization "wave" of the 1980s and 1990s, Western governments conformed to the business logic of the private sector in producing and providing goods and services, but also to the PPP doctrine, indicating a long-term contractual agreement between private and public actors to build or manage critical infrastructures or provide services for public utilities.

While PPP has been heralded as a "revolution" for infrastructures (Grimsey and Lewis 2004), results in terms of efficiency and accountability, however, have been mixed at best (Forrer et al. 2010; Andersson and Malm 2006; Hodge and Grebe 2007). Enthusiasm for PPP in critical information infrastructures (CII), including those of outer space, remains strong, however. Public and private actors involved in CII are struggling not only with technological reliability, but also with securing long-term investments, and how to make CII resilient (Wettenhall 2003). Moreover, organizational theories suggest that institutional fragmentation – i.e. too many stakeholders – negatively affects the ability to reliably manage critical systems, with possibly catastrophic consequences (Perrow 2011).

Major disruptions of critical information infrastructures would indeed have serious consequences not only for the public and private actors directly concerned, but also for the well-being and prosperity of possibly millions of people affected. Proper attention to security and safety, however, is sometimes lacking (Bailes and Frommelt 2004), due in part to the dominant techno-optimistic perspective on space and cyberspace technology. Indeed, relevant literature (Dunn Cavelty and Suter 2009; Newlove et al. 2018) shows that the relationship between the private sector and security is, mildly put, "problematic". Unsurprisingly, since security is the archetypical *externality*, economists have been wary about tackling it (Goodwind 1991). Security is a "large state-sector" and a public service for which economic models display an irritating unfitness. Likewise, "cybersecurity is a public good, which implies that without government intervention, it will not be produced" (Van Eeten and Bauer 2009: 230). As cyberspace moves to space, i.e. into another critical security domain, public and private stakeholders should rightly be concerned, particularly if lessons can be learned from the experience of cybersecurity and other critical information infrastructures with the help of the private sector. That public-private partnerships are indeed becoming major nexuses of space infrastructure is undeniable, particularly in Europe and North America (cf. Mörth 2007; Newlove-Eriksson and Eriksson 2013).

Interplanetary cyberspace?

While ideas of space colonization have influenced space policy since the beginning of the space age, they have recently gained new momentum. In 2015 NASA launched a new Mars settlement project, called "Journey to Mars", including the building of a new launch system (SLS), and a new spaceship called Orion. The timeline of NASA's space settlement project, like that of others, seems to have constantly moved forward. In 2015, NASA believed they would send the first crew to Mars sometime in the 2030s. In 2018, the plan has been moved forward, with a first crewed mission taking place in the 2040s, or later. This is partially due to President Trump's recently stated intention to first return to the Moon, and build a base there, before eventually going to Mars.

Among a handful of private initiatives for space colonization, the most well-developed project is that of SpaceX. Since 2011 SpaceX is *inter alia* delivering cargo to the International Space Station on its Dragon vessel. Yet, since the company was founded in 2002, the goal has been much more ambitious, i.e. to make humanity a "multi-planetary race", starting with the colonization of Mars. In 2016, SpaceX declared that it would send a first crew to Mars already by 2024. While the capability of SpaceX to build and launch rockets is undisputed, it is more uncertain if they will be able to send humans to Mars before the end of 2020s, especially as Musk himself has declared that his timelines are sometimes a little optimistic. SpaceX is currently developing a new large and reusable rocket system for interplanetary travel, the so-called Starship. In September 2018, SpaceX announced that the first version of this ship would carry the world's first space tourist – Japanese businessman Yuzaka Maezawa and a small group of friends – on a trip around the Moon in 2023. Other private initiatives for human space exploration include those of Orbital, Boeing, Blue Origins, Lockheed Martin, and Virgin Galactic. Likewise, in co-operation with Lockheed Martin, NASA is building its own rocket for deep space travel, the so-called Space Launch System and the associated Orion capsule.

Moreover, China, which has sent its own taikonauts to a temporary space lab orbiting Earth, has expressed visions of human space exploration far into the galaxy and beyond. Russia – which maintains the Soviet space infrastructure in Kazakhstan – has also stated long-term goals of human presence in space. Likewise, Japan, Canada, India, and a few other states have similar ambitions, although on a smaller scale. The European Space Agency has also stated intentions to join or develop their own human space exploration and has successfully reached far out in the solar system with unmanned probes, including Rosetta – the first human-made object to land on an asteroid. Even the United Arab Emirates – as part of a general mission to become an advanced high-tech country – have stated the goal of building cities on Mars within "the next hundred years".

Whether the exploration of human space continues in the form of settlements or even cities on other planets, or in the form of new free-moving or orbiting space stations – some form of *deep space communications system* is necessary. Space communications technology is rapidly evolving, with experimentation including not only radio signals but also lasers and optical systems. NASA's Jet Propulsion Laboratory, for example, is currently working on systems for internet-like space communication, capable of transmitting high volumes of traffic. This could very well be the first steps toward an interplanetary cyberspace.

The technological aspects of interplanetary cyberspace are discussed in a growing body of scientific and expert literature. This literature has addressed specific problems of deep space communication that have to do with distance, reliability, and versatility (Akyildiz et al. 2003; Bucur and Iacca 2017). For example, while the current internet protocols are built on latency in milliseconds, an interplanetary cyberspace must tolerate latencies or disruptions of up to several hours. This requires creation of so-called Delay-Tolerant Networks (DTN). Also, if space settlements become a reality, space communications *infrastructure* must be developed. In addition to ground stations and satellites orbiting Earth, a network of transmitters and other forms of communications infrastructure needs to be put up in deep space. The currently existing Deep Space Network (DSN), run by NASA, consists of Earth-based radio antennas and dishes, located in California, Spain, and Australia. A similar network has been established in 2013 by the European Space Agency, with antennas in Spain, Argentina, and Australia (Voosen 2016). Earth-based networks are clearly insufficient to support interplanetary settlements.

It is possible that some form of interplanetary internet-like communications system will develop, but it remains to be seen if there will be one or more versions of interplanetary cyberspace, and it is unknown how issues such as connectivity, access, security, privacy, and governance will be dealt with. Will deep space cyberspace be made secure with encrypted communications, or will it be easy to tap? Will there be a new cosmic digital divide? Who or what will govern intergalactic cyberspace? What norms and principles will cyberspace in space be based upon? If anything, the development of an Interplanetary cyberspace is plagued with a great deal of uncertainty –in terms of whether and how it will come about, what capacity and functions it will have, who will build it, and how it will be governed.

To be sure, the making of cyberspace in space requires connectivity also between current internet governance and space governance. ICANN and UNOOSA, for example, currently seem to have very little to do with each other. That might, or even should, be changing.

Conclusion: Fragmentation, vulnerability, and uncertainty

The development of cyberspace in space has two main drivers. The first is obviously the technological advances, which – similar to the development of computers – have made satellites both smaller and cheaper, yet at the same time more powerful and efficient. So-called nano-satellites are rapidly filling the skies, providing an increasing number of services – including cyberspace access – for a wide variety of clients including government, military, business, research, transport, NGOs, and individuals.

The second driver of cyberspace in space is the multiplication of space actors – both private and public, as well as different forms of public-private constellations. Privatization and liberalization of access to space, particularly in the United States but also elsewhere (e.g. Luxembourg) has opened up space for new types of private actors, not only "aerospace" and rocket companies, but also internet and new media companies (e.g. Google), as well as mining corporations, and even NGOs.

The development of cyberspace in space has three major consequences, which sums up the main observations made in this chapter. First, it implies *fragmentation* – particularly in terms of stakeholders and governance. It is likely that "governments will not hold complete control over technology dissemination in the global market" in space, something which is already the case for much of cyberspace (Harrison et al. 2017: 1). The growth of states with space program has gone from the original 2 to around 70 today, and the simultaneous growth of private corporations (and NGOs) in space contributes to an increasingly fragmented field of stakeholders. Fragmentation also applies to governance, which already characterizes the two still separate fields of cyberspace and space. Fragmentation will likely increase as these two fields merge. Comprehensive legal frameworks and mechanisms for conflict management and allocation of accountability are lacking, and the few elements that exist were developed during an earlier period, before privatization of cyberspace and space, the Internet of Things, and the renewed programs for space colonization.

Second, *vulnerability* is increasing. When cyberspace becomes increasingly reliant on space-based infrastructure, it becomes vulnerable to new types of threats (in addition to the more well-known dangers that threaten cyberspace on Earth) – not only deliberate attacks such as the use of anti-satellite weapons and targeted satellite hacking, but also the hazards of space debris and solar storms. Moreover, when some form of cyberspace eventually moves into the galaxy, for example when communications is set up between Earth and a remote space settlement, massive time lags and interruptions are to be expected. Programs for "space situational awareness" and the cleaning up space debris are helpful, but they are limited both in terms of participation and resources.

Third, *uncertainty* will be a prevailing feature for the foreseeable future, particularly concerning norms and principles of space activities, and what "balance of power" (if any) there will be in space. This could of course be said about current developments on Earth as well, yet there it is still possible to discern the relative power and influence of particular stakeholders and positions, for example regarding "Internet freedom" and "Internet sovereignty". With regard to cyberspace in space, however, developments seem even more contradictory and uncertain. Will the contradictory trends of, on the one hand, militarization and, on the other hand, civilian or even utopian visions of peaceful space exploration prevail, or will one type of future dominate – whether dark or bright? Looking beyond the horizon currently yields more questions than answers. Yet that uncertainty makes fertile ground for pioneers and adventurers, and many of them are found at the interface of space and cyberspace.

Finally, in order for social scientists to be able to track the development of cyberspace in space and analyze consequences for politics and security, familiarization with technical development and expertise is essential. Reading of expert articles on satellites and other infrastructures is of importance, as are efforts to bridge the gap between technical and social science expertise, which certainly has its challenges given differences in incentives and epistemic cultures. The latter is a prevailing challenge, which students of STS (Science and Technology Studies) have known for decades. Moreover, case studies and comparative analyses of internet satellite programs are of importance for gaining knowledge about the patterns of change and continuity in this field. In addition, analyses of the linkages and gaps between space governance and internet governance are particularly warranted.

References

All links checked on August 20, 2021.

Akyildiz, I. F., Akan, Ö. B., Chen, C., Fang, J., and Su, W. (2003). InterPlaNetary Internet: State-of-the-Art and Research Challenges. *Computer Networks*, 43(2): 75–112.

Amos, J. (2019). SpaceX Puts Up 60 Satellites. *BBC News*. Retrieved September 26, 2019, from: https://www.bbc.com/news/science-environment-48289204.

Andersson, J., and Malm, A. (2006). Public–Private Partnerships and the Challenge of Critical Infrastructure Protection. In M. Dunn and V. Mauer (eds), *International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects*. Zurich: Swiss Federal Institute of Technology, pp. 139–167.

Araxia Abrahamian, A. (2017, September 15). How a Tax Haven is Leading the Race to Privatise Space. *The Guardian*. Retrieved September 26, 2019, from: https://www.theguardian.com/news/2017/sep/15/luxembourg-tax-haven-privatise-space.

Bailes, A., and Frommelt, I. (eds). (2004). *Business and Security Public-Private Sector Relationships in a New Security Environment*. New York: Oxford University Press.

Bucur, D., and Iacca, G. (2017). Improved Search Methods for Assessing Delay-Tolerant-Networks Vulnerability to Colluding Strong Heterogeneous Attacks. *Expert Systems with Applications*, 80(1): 311–322.

Choudhury, S. R. (2019, July 22). Super-Fast Internet from Satellites is the Next Big Thing in the Space Race. *CNBC*. Retrieved September 26, 2019, from: https://www.cnbc.com/2019/07/22/fast-internet-via-satellites-is-the-next-big-thing-in-the-space-race.html.

Dunn, M. (2006). Understanding Critical Information Infrastructure: An Elusive Quest. In M. Dunn and V. Mauer (eds), *International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects*. Zurich: Swiss Federal Institute of Technology, pp. 27–53.

Dunn Cavelty, M., and Suter, M. (2009). Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4): 179–187.

Durst, R. C., Miller, G. J., and Travis, E. J. (1997). TCP Extensions for Space Communications. *Wireless Networks*, 3(5): 389–403.

Forrer, J., Kee, J. E., Newcomer, K. E., and Boyer E. (2010). Public-Private Partnerships and the Public Accountability Question. *Public Administration Review*, 70(3): 475–484.

Giacomello, G. (2005). *National Governments and Control of the Internet: A Digital Challenge*. London and New York: Routledge.

Giacomello, G. (ed.). (2013). *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*. New York: Lexington Books.

Goodwin, C. D. (1991). *Economics and National Security: A History of Their Interaction*. Durham and London: Duke University Press.

Grimsey, D., and Lewis, M. K. (2004). *Public Private Partnerships: The Worldwide Revolution in Infrastructure Provision and Project Finance*. Cheltenham: Cheltenham: Edward Elgar.

Gross, G. (2018, March 30). SpaceX Gets US Approval to Launch Space-Based Broadband Service. *Internet Society Blogpost*. Retrieved September 26, 2019, from: https://www.internetsociety.org/blog/2018/03/spacex-gets-us-approval-launch-space-based-broadband-service/?gclid=EAIaIQobChMIq6Phu97c5AIVhdGyCh36jQFrEAAYAyAAEgKHyfD_BwE.

Harrison, T., Hunter, A., Johnson, K., and Roberts, T. (2017). *Implications of Ultra-Low-Cost Access to Space*. Lanham: Rowman and Littlefield.

Hodge, G. A., and Greve, C. (2007). Public–Private Partnerships: An International Performance Review. *Public Administration Review*, 67(3): 545–558.

Jakhu, R., and Pelton J. (eds). (2017). *Global Space Governance: An International Study*. Cham: Springer.

Lin, J., and Singer, P. W. (2018, February 13). China Shot Down Another Missile in Space. *Popular Science*. Retrieved September 26, 2019, from: https://www.popsci.com/china-space-missile-test.

Liou, J. C., and Portman, S. (2007). Chinese Anti-Satellite Test Creates Most Severe Orbital Debris Cloud in History. *Orbital Debris Quarterly News (NASA)*, 11: 2–3.

Martinez, L. F. (1998). Satellite Communications and the Internet: Implications for the Outer Space Treaty. *Space Policy*, 14(2): 83–88.

Mörth, U. (2007). Public and Private Partnerships as Dilemmas between Efficiency and Democratic Accountability: The Case of Galileo. *Journal of European Integration*, 29(7): 601–617.

Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Oxford: Polity Press.

Newlove-Eriksson, L., and Eriksson, J. (2013). Governance beyond the Global: Who Controls the Extraterrestrial? *Globalizations*, 10(2): 277–292.

Newlove-Eriksson, L., Giacomello, G., and Eriksson, J. (2018). The Invisible Hand? Critical Information Infrastructures, Commercialization, and National Security. *The International Spectator*, 53(2): 124–140.

Perrow, C. (2011/1984). *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press.

Rosone, J., and Watson, M. (2017). *Cyber Warfare and the New World Order: World War III Series*, Book IV. Independently published.

Rothe, D., and Shim D. (2018). Sensing the Ground: On the Global Politics of Satellite-Based Activism. *Review of International Studies*, 44(3): 414–437.

Slann, P. A. (2016). Anticipating Uncertainty: The Security of European Critical Outer Space Infrastructures. *Space Policy*, 35(February): 6–14.

Stephens, D. (2017). Increasing Militarization of Space and Normative Responses. In R. Venkata Rao, V. Gopalakrishnan, and K. Abhijeet (eds), *Recent Developments in Space Law*. Singapore: Springer, pp. 91–106.

Valeriano, B., Jensen, B., and Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Van Eeten, M., and Bauer J. M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management*, 17(4): 221–232.

Voosen, P. (2016). Deep Space Network Glitches Worry Scientists. *Science*, 353(6307): 1477–1478.

Walsh, D., and Suliman, A. Z. (2018, September 4). A Facebook War: Libyans Battle on the Streets and on Screens. Retrieved from: https://www.nytimes.com/2018/09/04/world/middleeast/libya-facebook.html.

Wettenhall, R. (2003). The Rhetoric and Reality of Public-Private Partnerships. *Public Organization Review*, 3(1): 77–107.