Cyber Security Governance and the Theory of Public Goods

https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/

MISCHA HANSEL, JUN 27 2013

Cooperation in cyber security is a difficult task even in the absence of national security considerations. Actions in cyberspace create numerous ambiguities, cause-effect relations span the whole globe and attribution of responsibility is often not possible. Once states participate in cyber security governance, however, collective action problems may become particularly severe. This article discusses international cooperation problems and institutional remedies by applying the theory of public goods. Its main conclusions are as follows: Whereas genuine free riding temptations pose only modest risks to cyber security governance, weak cyber defences create significant externalities and can therefore be understood as a global public bad. What may be required to improve this state of affairs is a future regime that combines 'sticks' and 'carrots' and, thus, changes state incentives.

Cyber Security and the Theory of Public Goods

Daniel Kuehl defines cyberspace as a "global domain […] whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum [to create, store, exchange, and exploit digital data via] interdependent and interconnected networks" (Kuehl 2009: 28). Cyber security, as it is understood here, denotes the availability, integrity, authenticity and confidentiality of the digital data stored in and transmitted through cyberspace. Cyber security policies can be based on unilateral or multilateral measures. As long as the majority of actions in cyberspace tend to ignore physical boundaries, unilateral efforts tend to be costly or inefficient. While states can always cut themselves off the internet, this option almost certainly entails high economic costs. During the one-week internet blackout in Egypt in 2011, which the government intentionally brought about, the Egyptian telecommunication industry lost an estimated revenue of 90 to 110 million US dollars.

If isolation is not a viable option then cooperation is essential for ensuring cyber security. Even the most capable state simply cannot hope to anticipate and fend off all cyber attacks on its own. Cooperation can occur ad hoc or on a regular basis. Studies of global governance are usually concerned with the latter type of cooperation (see Karns/Mingst 2004). According to this understanding cyber security governance comprises voluntary cooperative efforts to ensure the availability, authenticity, integrity and confidentiality of digital data stored in or transmitted through cyberspace.

The aim of this article is to demonstrate the usefulness of the theory of public goods, a framework that originated in economic sciences, for understanding the challenges of cyber security governance. Global public goods, such as the ozone layer, the absence of war or the co2-absorbing effects of rain forests, are non-rivalrous and non-excludable. Non-rivalry means that consumption of the good by one actor does not result in the reduction of the overall availability of the good. Non-excludability refers to the practical impossibility of excluding any actor from consuming the good (see Samuelson 1954: 387-389). Public goods create both favourable and unfavourable conditions for collective actions (see Olson 1965). On the one hand the continued provision and protection of public goods is in everybody's interest. On the other hand it is possible to lean back and to let others do the job while still benefiting from the provision of public goods. The temptation to exploit the efforts of others creates the problem of so-called free-riders (Samuelson 1954). It is because of the existence of such free-riders that public goods tend to be underprovided (see Boyer/Butler 2005: 75-91). The greater the number of actors, the stronger is this tendency (Olson 1965: 48). The

under-production of public goods is quite common in international relations (see Sandler 1997). It can be avoided in two different ways: There has either to be a single state or a group of states that are willing to bear additional costs by making an extra effort in terms of public good creation (Olson 1965: 49-50; Kindleberger 1981; Gilpin 1981: 138-139, 144-145). Alternatively states manage to establish an international regime which is able work as a disincentive to free-riding by facilitating the identification and punishment of free-riders (see Keohane 1984).

Cyber Security Governance as a Free Riding Problem

Is cyber security a public good? It is certainly not a pure public good. Most goods in international relations are not (see Boyer and Butler 2006: 76). A state who invests in its cyber defence, first and foremost, improves the security of its own public or private networks (i.e. those networks under its jurisdiction). Yet to a certain degree it also benefits other states' cyber security. We used to think of computer networks primarily as a target of cyber attacks, but they just as well serve as 'stepping stones' or 'spring boards' for attacks on third parties. Attackers 'steer' their malware through several networks and jurisdictions in order to cover their tracks. Strongly guarded computer networks, therefore, contribute to cyber security system-wide to a certain degree. Weakly defended computer networks, in turn, do not cause a risk to their proprietor alone but also to other networks. They may even solely risk the security of other networks in case the weakly guarded network itself does not harbour anything of enough economic or political value. Weak cyber security, in this view, is a so-called public bad just like carbon dioxide emissions or deforestation. Virtually nobody is excluded from its effects and its proliferation does not slow down with the number of actors suffering from it. It should be added that weak cyber defences are not only caused by technical and organizational but also by legislative deficiencies. A good example is the so-called I-love-you virus of 2000, a computer virus that led to financial losses in the amount of several billion US dollars worldwide. After law enforcement agencies finally identified the creator of the virus, a young student from the Philippines, they could not arrest and prosecute him because Philippine law did not prohibit the creation and use of computer malware at that time.

It should be emphasized here that whereas Philippine law did weaken national cyber security the Philippines themselves did not fall victim to these deficiencies. Rather the leading economies in America, Western Europe and East Asia suffered from the damage to essential IT-systems. The case of the I-love-You virus therefore exemplifies a general pattern: poor states have fewer incentives to invest in cyber security than rich states. As long as every state independently provides for the security of its own networks, and according to its own interests, it is very likely that cyber security as a public good is under-provided on a global level. How can the global under-provision of cyber security be avoided? Coming back to what has been said at the beginning of this article there are basically two possibilities. One is the creation and enforcement of an international regime that effectively punishes those who fail to meet a certain standard of cyber security. The other possibility is that a group of stronger states voluntarily provides 'cyber security aid' to weaker states. The first strategy has been discussed primarily in the US. The second is already pursued in various bilateral and multilateral frameworks.

Sovereign Responsibility and Cyber Security Aid

Both the "Cyberspace Policy Review" of 2009 (p. iv.) and the US "International Strategy for Cyberspace" of 2011 (p. 8) argue for the establishment of a new international norm that would make states responsible for whatever cyber attacks come from infrastructures under their jurisdiction. The idea is to work around the problem of attribution. Norms of „sovereign responsibility" (p. iv.) would commit each and every state to prevent its national networks from becoming safe havens for cyber criminals and other attackers. By the same token states could no longer hide their own campaigns behind supposedly private hackers. Some US officials and commentators even push for more radical ideas by advocating sanctions or legitimizing 'hacking back' tactics in case of norm violations. According to Michael Hayden, the former director of the National Security Agency (NSA), internet traffic from and to deviant states could be slowed or even cut off. Similar ideas are presented by former cyber security advisor to the White House Richard A. Clarke (Clarke and Knake 2010: 249-255). Already in 2008, Colonel Charles W. Williamson III called for a military botnet that could be used in self-defence against attacks even from neutral or allied nations. International law already provides enough justification for such 'active defense' measures argues Matthew J. Sklerov, a Department of Defense official (Sklerov 2010). As long as the state from which jurisdiction the attacks are coming is either unwilling or unable to stop the attacks itself the victim can legitimately 'hack back'. It does not have to prove the cognizance or

complicity of the state which sovereignty it is going to injure. By the same logic the UN Security Council authorized the US military actions against the Taliban government in Afghanistan (Sklerov 2010: 53-57, 64-65). A similar regime in the issue area of cyber security would almost certainly dissuade states from not caring for the protection of their IT-infrastructure. However, Sklerov also admits that current state practices as well as the majority of international law experts do not support the same reasoning in cyberspace yet (Sklerov 2010: 62).

A second solution to the problem of free riders or public bads consist of a single state or a group of states providing 'cyber security aid' to those states with weak cyber defence policies and capabilities. Those who have a special interest in a high level of cyber security could offer technical or legal advice. Alternatively they could even take over the protection of foreign networks just like the US took over most of the protection of Western Europe during the Cold War. Empirically there are examples of the first variant but not of the second. The reason seems to be simple. Whoever defends foreign networks can also exploit foreign networks because the very same knowledge enables both defensive and offensive actions. Moreover, since warfare, crime and intelligence are hard to distinguish in cyberspace, the protecting power could at the same time fend off cyber attacks of a third party and prepare for its own espionage activities. Hence, probably very few states are willing to compromise their national security in a way that would make possible security umbrellas in cyberspace.

In contrast the advancement of cyber security via technical and legal aid is a low-risk model from the perspective of those on the receiving end. It has been already practiced on a bilateral and multilateral basis. Amongst the most active cyber security aid providers is the United States. The rationale used to explain these policies is intimately connected with the idea of a benign hegemon and public good provider:

"In an interconnected global environment, weak security in one nation's systems compounds the risks to others (International Strategy for Cyberspace, p. 19)."

"[…] As the world's leading information economy, the United States is committed to ensuring others benefit from our technical resources and expertise. Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems (International Strategy for Cyberspace, p. 14)."

In keeping with these commitments organisational branches of the Department of Commerce and the Department of Homeland Security help Latin American and Caribbean states to acquire technical, regulative and administrative capacities in the framework of the Organisation of American States (OAS). The US Justice Department participates in training programmes for APEC and ASEAN members as well as for member states of the African Union and ECOWAS. The Bureau of Intelligence and Research (BIR) of the US State Department provides expertise in the framework of the OSCE. Despite these and other activities which were welcomed in a report by the US Government Accountability Office, experts and parts of the administration regularly call for a more comprehensive cyber aid program (see, for instance, Lord and Sharp 2011: 41).

Besides the US and other major cyber powers international organisations are central actors in the new business of cyber security aid. The International Telecommunications Unions (ITU) Global Cyber Security Agenda (GCA) is committed to the improvement of state and private capabilities around the globe (see Sofaer, Clark and Diffie 2010: 186-187; Portnoy and Goodman 2009: 11-18) and developing countries can participate in the „ITU Cybersecurity Work Programme to Assist Developing Countries". In the framework of the European Union, the European Network and Information Security Agency (ENISA) assists public and private actors with the establishment and operation of Computer Emergency Response Teams (CERTs). Experts and decision-makers nevertheless complain about enduring capability gaps. Many developing and newly industrialized countries are lagging behind in terms of the installation of sensors and the procurement of computer forensic devices. According to US officials (see GAO, p. 36-38) some countries still do not care about cyber security and/or lack the technical capabilities required to operate their own CERT. Even among European countries capabilities are still unevenly distributed according to German security officials (personal interviews). It is obviously still a long way to go before cyber security aid will become a widely-used and efficient tool. In the meantime an international regime based on the concept of sovereign responsibility may appear as a more attractive alternative.

Cyber Security and Internet Freedom

Some final remarks as to the interdependencies between cyber security and other political goals may be appropriate here. How can the US and other democratic powers ensure that cyber security aid to authoritarian regimes is not used to observe and intimidate political dissidents? Western companies and technologies already play a key role in the surveillance and censoring of internet communication all over the world. Many argue for tighter export controls in that area. This raises the question of whether we have to think of US cyber security aid programs and the US internet freedom agenda as complementary or contradictory efforts (on this point see Fontaine and Rogers 2011)? Are there any viable safeguards against the misuse of cyber security aid? Are such safeguards possible at all? Suffice to say that, time and again, cyberspace blurs concepts and agendas that we are used to think of as being separated. Perhaps this feature more than any other makes the business of international cooperation in the issue area so much complicated.

—

Mischa Hansel *is an Assistant Professor at the Institute for Political Science and European Affairs at the University of Cologne. His dissertation on international cyber-security cooperation was supported by a research grant from the Konrad-Adenauer Stiftung (KAS) e.V. He worked as a Research Fellow at the German Armed Forces and Staff Academy (Führungsakademie der Bundeswehr) in Hamburg, the Elliott School of International Affairs at George Washington University (GWU) and the European Space Policy Institute (ESPI) in Vienna. He has also taught at the Cologne School of Journalism and Matej Bel University in Banská Bystrica (Slovakia). His research interests include security regimes and arms control, internet governance, the United Nations, Indian foreign policy, the Global South and human rights.*

The author would like to thank Jamal Shahin, Joachim Alexander Koops and Benjamin Robin Barton for their comments on an earlier draft. All remaining errors are naturally my own.

References

Boyer, Mark A. and Butler, Michael J. (2006): Public Goods Liberalism: The Problems of Collective Actions,"in: Jennifer Sterling-Folker (ed.): *Making Sense of International Relations Theory*, Boulder/London: Lynne Rienner, 75-91.

Clarke, Richard A. and Knake, Robert K. (2010): *Cyberwar: The Next Threat to National Security and What to Do about It*, New York: Harper/Collins.

Fontaine, Richard and Rogers, Will (2011): Internet Freedom and its Discontents: Navigating the Tensions with Cyber Security, in: *America's Cyber Future: Security and Prosperity in the Information Age* , Volume II, Washington, DC: Center for a New American Security, 145-164.

Gilpin, Robert (1981): *War and Change in World Politics*, Cambridge: Cambridge University Press.

Karns, Margaret P. and Mingst, Karen A. (2004): *International Organizations: The Politics and Processes of Global Governance*, Boulder et al.: Lynne-Rienner.

Keohane, Robert O. (1984): *After Hegemony: Cooperation and Discord in the World Political Economy* , Princeton: Princeton University Press.

Kindleberger, Charles P. (1981): Dominance and Leadership in the International Economy: Exploitation, Public Goods and Free Rides, *International Studies Quarterly* 25(2): 242-254.

Kuehl, Daniel T. (2009): From Cyberspace to Cyberpower: Defining the Problem, in: Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds): *Cyberpower and National Security*, Washington, DC: National Defense University

Press, 24-42.

Lord, Kristin M. and Sharp, Travis (2011): *America's Cyber Future: Security and Prosperity in the Information Age* , Volume I, Washington DC: Center for a New American Security.

Olson, Mancur (1965): *The Logic of Collective Action: Public Goods and the Theory of Groups* , Cambridge: Harvard University Press.

Portnoy, Michael and Goodman, Seymour (2009): *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, Vienna/New York: Springer.

Samuelson, Paul A. (1954): The Pure Theory of Public Expenditures, *Review of Economics and Statistics* 36(4): 387-389.

Sandler, Todd (1997): *Global Challenges: An Approach to Environmental, Political, and Economic Problems* , Cambridge: Cambridge University Press.

Sklerov, Matthew J. (2010): Responding to International Cyber Attacks as Acts of War, in: Jeffrey Carr (ed.):*Inside Cyber Warfare*, Sebastopol: O'Reilly Media, 45-75.

Sofaer, Abraham D./ Clark, David and Diffie, Whitfield (2010): *Cyber Security and International Agreements, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington DC: The National Academies Press.

About the author:

Mischa Hansel is an Assistant Professor at the Institute for Political Science and European Affairs at the University of Cologne. His dissertation on international cyber-security cooperation was supported by a research grant from the Konrad-Adenauer Stiftung (KAS) e.V.. He worked as a Research Fellow at the German Armed Forces and Staff Academy (Führungsakademie der Bundeswehr) in Hamburg, the Elliott School of International Affairs at George Washington University (GWU) and the European Space Policy Institute (ESPI) in Vienna. He has also taught at the Cologne School of Journalism and Matej Bel University in Banská Bystrica (Slovakia). His research interests include security regimes and arms control, internet governance, the United Nations, Indian foreign policy, the Global South and human rights.