Student Number: 677056

What are the respective roles of state and non-state institutions in socio-technical security provision in anarchy? Analysis of today's security provisions to identify security-relevant developments in today's socio-technical societies, where isolated analysis of physical and cyber security is not indicative.

MSc Global Corporations and Policy (Online)
Center for International Studies and Diplomacy
School of African and Oriental Studies

Word Count: 14999
5 October 2021

This dissertation is submitted in partial fulfilment of the requirements for the degree of MSc Global Corporations and Policy (Online) of the School of Oriental and African Studies (University of London)

Abstract

Today, the UN-Charter-derived sovereign states' dominance in anarchy is taken for granted, including their constituting institutions. Much research addresses technology and Internet challenges. However, current research and existing theoretical foundations focus on how sovereign states can address these challenges, presuming that sovereign states and their constituting institutions (e.g., geographically-separated states, "traditional" separations of power) are suitable to handle these challenges. Yet, past international systems often lost their suitability when the world's conditions changed. More recently, the world's conditions changed again. Societies are no longer just social systems but socio-technical systems: the transitions and boundaries between real-world and cyber realms are fluid today. Impacts are reciprocal and omnipresent, without distinct transitions that could limit these impacts. Events in one realm affect both. This affects security provision, making social contracts to socio-technical contracts. However, legally-unprovable cyberattacks challenge the presumption of innocence while sovereign states struggle to develop, standardize and deploy secure IT infrastructures for their citizens: cyberattacks on states often exploit known (social or technical) vulnerabilities of software or software's socio-technical development/deployment environment. Yet, the Internet's complex globally-distributed infrastructure itself remains resilient, despite attractiveness for attackers: Linux kernel hacks could affect 51%-99.8% of the Internet's critical infrastructure servers, which "run the Internet" and process valuable data. However, Linux development, Linux's infrastructure-related deployments, and the operation/coordination of the Internet's sub-networks including technology standardization, are part of a transnational system with novel institutions avoiding social and technical abuse: the non-state institutional architecture that "develops and runs the Internet" remains largely self-regulated contributing to security provision in anarchy, where traditional state institutions struggle. My thesis focuses the respective role and behavior of today's institutions in socio-technical security provision in anarchy to identify false presumptions, indicate possible developments and indicate requirements for future socio-technical contracts: institutions make suitable socio-technical contracts and contract-implementing organizations, not vice versa.

In between cyber cultures and the international society

On one hand, most dominant institutions on the Internet manifest somehow in formal organizations, which are embedded in the international society's legal framework. Thus, it can be argued that there is a new system of institutions but it remains subordinated to the international society. However, although facilitated by legally-recognized organizations, the powerful communities remain independent from these legal entities. E.g., the Linux Foundation pays the leader appointed by the community, not vice versa. The community has already proven able to find sponsors to pay its leaders without a centralized organization: the community shapes norms and appointments, and there are no legal obligations for communities. This already starts with the global consent to use Linus Torvald's GitHub account for the Linux mainline kernel, making every derived kernel dependent on what he accepts in his repository.

Further, these informal institutions and entities outside the international society's framework have already challenged that society: this includes examples like SELinux, which had to be adjusted until the community accepted it, but also the Montevideo statement, which can be interpreted as warning against international society's tacit acquiescence to U.S. dominance among states in cyberspace, reminding that the Internet is only conditionally dependent on state-influenced institutions, able to replace them if this proves competitive. However, the entry barrier to the latter alternative is very high, and the resulting interaction with the international society cannot be foreseen, including the outcomes.

Maybe, the interaction of Internet-related MNCs like IBM, Google or Facebook with the international society prove indicative: on one hand, they have imposed many institutions on the world (e.g., social media, which shapes politics and privacy perceptions) and on the Internet (shaping technology developments like Linux). These MNCs shape imitation of behavior, which includes states, whose governments have to regulate but also engage themselves in social media to keep competitive. On the other hand, the European Union has proven to be capable to impose its norms internationally beyond its borders ("Brussels effect") such as the General Data Protection Regulation (GDPR), which has been adopted by entities on the Internet outside the EU (Gady,2014,pp.16-19). In the end, average citizens will make the difference: citizens are the environment that accepts or rejects institutions, and that accepts an entity as the sovereign or not. Yet, it remains open how their behavior develops.

Currently, it is possible to argue that there are already two international systems in anarchy, one "transnational system" that centers on the Internet but with real-world impact, and the traditional international society. Yet, it can be also argued that the first remains subordinated to the latter. The security provision in anarchy by the "transnational system" is a major problem if presuming the existing international society to be dominant: acceptance of a sovereign depends on citizen's perception of provided security, and if the transnational system on the Internet stops providing it while the international society remains unable to replace the transnational system, the legitimacy of sovereign states may be at risk because the security perception decreases. Then, citizens may seek a new, or a changed, sovereign offering that perception.

Finally, there is no evidence that traditional state institutions would be able to create security in Internet-related technology realms. However, a dominance takeover of the "transnational system" remains a probabilistic possibility but unproven either. Indeed, the informal elements of the transnational system can be questioned for their suitability in real-world scenarios. A third possibility that cannot be excluded is a rising bipolarity between two dominant systems in permanent interaction. The Wikileaks institution, whose origin cannot be traced back to a single one of the two systems, has been indicative for conflicts between the systems, especially through Edward Snowden's papers. Indeed, Wikileaks and the normalization of whistleblowing illustrate the competitive institutional alignment between two incompatible systems within an environment of citizens with dissonant perceptions in terms of security needs and legitimate institutions.

Chapter V. Conclusion

My research aimed to identify the role and behavior of state and non-state institutions in "socio-technical contract"-relevant security provision and their relation to each other, unbiased from the presumption that security provision implies state institutions. My goal was to identify the presumption that security provision is and remains the unchallenged domain of the UN-charter-derived sovereign state as false. Thus, I wanted to identify the need for investigating alternative future developments, next to the possibility of the international society to remain dominant.

Social contracts need a physical capability as foundation, but they also depend on the citizen's perceptions. The Internet is real-world-dependent. However, sovereign states have their dependencies, too. Indeed, MNC's and Internet-risen entities have already imposed their will on sovereign states and made them compete in favor of these non-state actors' interests, but also vice versa. People depend on geography, which makes geography integral part of security provision. However, people, their jobs, companies and other entities especially in industrialized states also depend on the Internet today: that includes sovereign states, which have to use and engage in cyber space to offer competitive socio-technical contracts. Societies have become socio-technical: the transitions and boundaries between real-world and cyber realms are fluid today; there is no explicit point of transition where impacts could be limited. Impacts are reciprocal and omnipresent. Events at one realm affect both. Socio-technical contracts have to adjust to this fact, and although past experiences of what institutions are suitable/competitive in social contracts remain valuable indications, they have not yet proven suitable for today's socio-technical contracts.

Indeed, it can be argued that there is already an alternative, transnational system that establishes order in many socio-technical areas of anarchy. Sovereign states already depend on the contribution to security provision by online-communities and transnational organizations on the Internet: the impact of a hacked Linux kernel or misconduct (including loss of trust) in the ICANN or IETF would set the social contracts of sovereign states at risk because it could impair operations of and on the Internet, including all dependent users/citizens/organizations, and thus, impair socio-technical security.

On the Internet, many competitive institutions have risen to create order in anarchy. Further, some of these institutions fulfill a comparable role as the real-world's separations of power but are competition-based: open and public data/information as well as widespread distribution (not separation) of powers (including widespread capacities to take over powers) are important institutions, collectively enabling "forking" and therefore, ensure stable competition-equilibria and avoid monopolies or power centralization. These institutions are complemented by low entry barriers to participate in an entity's activities. Forking and openness of code, debates and decision-making have been established as fundamental rights/institutions in security-related fields on the Internet. Merit-based influence capabilities of members and the informal derivations of rough consensus contribute to efficient and qualified decision-making. However, these institutions' informal and probabilistic characteristics can be questioned for their real-world suitability, outside cyberspace, because in real-world social contracts, more formal and distinct characteristics have prevailed over time.

Currently, there are state and non-state institutions that provide security in anarchy. However, the NIST is an example of state entities to adopt non-state institutions. Thus, institutions indicate how future socio-technical contracts might look like, but not which entities will hold and fulfill these contracts. The latter can barely be predicted with reasonable certainty so far, although knowledge of institutional developments facilitates such analyses. Indeed, my research determined several realistic possibilities of the sovereign states to remain dominant (through the international society, or bi-/multilateral): being false presumptions does not imply that these possibilities were disproved but that they are not the sole possibilities. Alternatively, the transnational system on the Internet might gain influence in anarchy. This can imply taking over dominance, or establishing bipolarity in anarchy through a second system next to the existing one.

Due to the far-reaching and complex interrelationships, entanglements, opportunities and related institutions and organizations, parts of my thesis may be considered selective. However, in this field, there is a lack of both theoretical and factual knowledge due to the lack of research: there is currently no theoretical foundation for cohesive research in this field. Yet, my goal was to indicate potential alternative developments, not prove any one of them. Thereby, my goal was to also identify the existing presumptions, which are the only ones that have received significant research, as false: they are possible but not proven. The institutions I identified are in place and provide security as of today, indicating suitable features for competitive future socio-technical contracts and indicating directions for future research, which have been neglected so far. The mere possibility of alternatives proves that the existing presumptions of the enduring suitability/competitiveness of traditional institutions and entities are only unproven possibilities among others. Research has to be more open-minded in challenging presumptions to evaluate developments without biases.

Technologies like Linux, their development and their institutional architectures need consideration in security research, just like military technologies, capabilities, and structures: their impact on socio-technical security provision can be comparably critical. ICANN, IETF, Linux-related communities and their institutions already provide security where sovereign states are (at least for now) incapable.

The research of institutions should be given special emphasis, as institutions are key factors: institutions make and shape both the competitive socio-technical contracts and the contract-implementing organizations, not vice versa. Also, focusing institutions reduces the risk of a human weakness in probabilistic matters to affect research or decision-making: entities/organizations develop too quickly into constructs that are taken for granted, no longer questioned in their agency.