The Politics of Cybersecurity: Balancing Different Roles of the State

Myriam Dunn Cavelty and Florian J. Egloff,
Center for Security Studies, ETH Zürich

Abstract

In liberal democratic countries, the role of the state in cybersecurity is a politically contested space. We investigate that role along three dimensions: the first is ***theoretical*** *and we look at existing cybersecurity literature, showing that international affairs literature is almost exclusively highlighting the role of the state as a security actor. We argue that this view is too narrow and risks limiting the discussion to only a few aspects of what cybersecurity entails. The second is* ***empirical*** *and we analyse policy development, showing the diversity of the roles the state imagines for itself. The state occupies six different roles in cybersecurity: (1) security guarantor, (2) legislator and regulator, (3) supporter and representative of the whole of society, (4) security partner, (5) knowledge generator and distributor, and (6) threat actor. The third dimension is* ***normative*** *and we investigate what the role of the state should be. To do that, we outline three main areas of tension between the state, the economy, and society in which cybersecurity policies are situated. Diverse coalitions of interests, spanning across the three social fields, support or challenge the six roles. Thus, two types of questions occupy the centre stage of cybersecurity policy: a question regarding the boundaries of responsibility (i.e., where does the responsibility of the state, economic, and societal actors start and end?) and a question regarding the concrete assumption of responsibilities (i.e., which means is an actor allowed to use to assume the responsibilities of his/her roles?). In sum, our conceptualisation enhances the understanding of cybersecurity as a diverse and crosscutting policy field. The result is a more comprehensive understanding of different roles of the state, which will help researchers with finding innovative research questions in the future.*

Introduction

What is cybersecurity? What seems like a simple question is at the heart of the political challenge this issue has become. Exemplified in the difficulties many state actors confess to have when it comes to agreeing on official definitions,[1] cybersecurity is notoriously hard to pin down and is contested politically in both national and international arenas. In explaining the reasons for this contestation, we will advance a better understanding of what cybersecurity has become and will highlight the diverse roles of "the state" that have emerged.[2]

Myriam Dunn Cavelty and Florian J. Egloff, “The Politics of Cybersecurity: Balancing Different Roles of the State.” *St Antony’s International Review* 15 no.1 (2019):37-57.

One reason for the difficulty in defining cybersecurity to the satisfaction of different stakeholders is the continuing evolution of the concept. Not so long ago, cybersecurity – or rather, its predecessor concepts, such as critical information infrastructure protection or information security – used to be an issue primarily discussed in expert circles as a technical or risk management problem. Now it has become a national security issue dealt with in the highest government circles, not least due to a marked increase in strategically motivated state activity in cyberspace, which is itself a side effect of current geopolitical tensions.[3] High-level cyberincidents not only affect individuals or single businesses, but also are seen as a threat to states, societies, and economies. Consequently, states are reviewing their own offensive and defensive capacities and are consolidating their strategic planning regarding the use of cyberspace.[4]

However, cybersecurity is not only moving upwards in political agendas worldwide: parallel to the advancing digitalisation, which is reflected in the increasing computerisation and automation of processes in business and society, cybersecurity is also expanding as a problem area to a multitude of additional policy domains not traditionally within the narrow purview of security. Cybersecurity has become a new focal point for education and training of the cybersecurity workforce, makes an appearance as capacity building in development cooperation, has been linked to a new type of diplomacy in foreign policy, appears as cyber-mediation in conflict management, and, definitely not least, is considered an important business sector or, more generally, the backbone for economic viability in a digitalising world.[5] Thus, cybersecurity is at the same time becoming more important, more diverse, and more diffused.

These developments raise pertinent questions for research that we explore in this article: How should cybersecurity be understood to do justice to its current and future conceptualisation in policy debates and political practice? Given its diversity, what roles and responsibilities do different actors have for which aspects of the complex problem? And which contestations between different actors structure the cybersecurity policy field?

To highlight the political governance aspects of the issue, we put ‘the state’ at the centre of this investigation. Using bibliographical data, a comparison of policy documents, and country-related policy papers from an ongoing research project as our main empirical basis,[6] we show which different political functions the state is expected to perform in cybersecurity and which political and social problems arise as a result.[7] On the one hand, the article undertakes a conceptual sharpening by showing empirically what cybersecurity is from the state perspective. On the other, this article argues that cybersecurity must be understood in its multiple facets and as a cross-cutting policy field in which political trade-offs are necessary.

The roles of the state in cybersecurity can be investigated in at least three dimensions. A first dimension is *theoretical*. In what ways does the existing literature theorise the role of the state? A second dimension is *empirical*. It encompasses questions such as: What role does the state play in building cybersecurity as national security (both active and passive)? What other roles do states play today? What kind of institutions are there that deal with cybersecurity? What are their tasks? How do they work? What impact does the special way cybersecurity looks today have on societal security? The third dimension is *normative* and investigates the question of what the role of the state should occupy. We consider all three dimensions to be important and therefore dedicate a section to each of them.

In the first section on the theory, we focus on existing definitions of cybersecurity as well as on the literature on cybersecurity politics. We note that the cybersecurity literature in international relations and political science more generally looks at its topic almost exclusively as an international security problem. This, we argue, is too narrow. National cybersecurity strategies illustrate that cybersecurity touches a multitude of issues in different policy areas. In the second section, we therefore highlight manifold roles of the state, partly desired by the state itself and partly demanded from outside. We situate cybersecurity concerns as emerging from three areas of tension between state, economy, and society. This, we show, leads to political conflicts inside and outside the state on several levels, due to the varied interests of different stakeholder groups.

We conclude that cybersecurity policy encompasses problems in these three areas of tension that can only constructively be dealt with if different interests are understood and consciously balanced. Such a policy finds a balance between the thematic alliances existing in societies, the different departments of the state, and the various interest groups of the economy. Different visions of the role of the state are therefore reflected to varying degrees in the three areas of tension. Such an understanding provides a solid foundation for making strategic decisions, negotiating policy guidelines, and further researching the changing roles of the state around cybersecurity.

Given that cybersecurity is an empirically dynamic and fundamentally interdisciplinary issue, doing justice to the literature is not a banal undertaking. First, 'cybersecurity' is a relatively new term, coming into existence only around the year 2000.[8] Second, with origins in the computer sciences, cybersecurity has different meanings for different research communities. To get a better understanding of how the literature treats 'the state,' we first attempt to get an 'objective' overview that extends beyond our own disciplinary bias through using two of the most prominent scientific databases, World of Science (WoS) and Scopus.[9] Second, we dig deeper into the most cited articles[10] to identify the different roles of the state that make an appearance in the literature on an abstract level. Last, we look at how international relations literature has treated the subject to identify the most pertinent gaps.

Cybersecurity research across disciplines

The two prominent scientific databases, World of Science (WoS) and Scopus, show that from 2012 to 2014, the quantity of scientific output on 'cybersecurity' almost doubled. In both databases, computer science tops the list of research areas with a very high percentage (WoS: 72 percent / Scopus: 61 percent), followed by engineering on the second rank (WoS: 36 percent / Scopus: 40 percent).[11] All the top ten cited articles in both databases focus on smart grids and/or SCADA (Supervisory Control and Data Acquisition) systems, a category of software used in many industrial processes to control equipment and conditions. Though the larger backdrop of insecurity resonates with the national security narrative, the technical view on cybersecurity is predominant, with little to no interest to understand the threat context. The main aim of research is to develop better cyber incident prevention, protection, and detection capabilities on the one hand, and more 'resilient' systems and infrastructures, signifying timely recovery of functionality if under duress due to an attack, on the other. The role of the state is of very little to no interest in this literature.

Bibliographical data further reveals that social science research on cybersecurity issues is marginalised in comparison to research in the technical sciences. Scopus has 'social sciences' as a lump category in third place, with 18 percent, whereas WoS lists 31 percent of its cybersecurity records in the same category. There are two main focal points in top-cited research in the social sciences: the first is an interest in organisational and managerial aspects of cybersecurity, like 'information sharing' between state and private actors[12] or the combination of technology with human and organisational factors.[13] The state, argues the general opinion in the literature, is incapable of providing the public good of security on its own, since an overly intrusive market intervention is a flawed and undesirable option. This opinion is based on the observation that what the state aims to protect due to national security considerations is also the foundation of the competitiveness and prosperity of a nation.[14] Hence, the state is treated as an important actor, while simultaneously there is much emphasis on the necessity to take into consideration the preferences of other actors.

The second focal point, fitting squarely into the 'international relations' sub-category, is the analysis of cyberwar and other threat forms. This literature aims to understand cybersecurity as a political phenomenon more generally, and specifically to understand how cybertechnologies change conflict dynamics, thus influencing the overall security in the international system. Before there were enough real-world cases to study, cybersecurity publications in this category focused primarily on cyberwar, especially the rhetorical hyperbole about it[15] or how best to fight wars in cyberspace.[16] Only more recently, traditional conflict research has started to look at the effect of cybertechnologies as tools in foreign policy and conflict using quantitative methods.[17] This type of research asks how and to what degree cyberspace as a domain of warfare influences (inter alia) coercion, offence-defence theory, and deterrence.

The focus is on how cybertechnologies become tools for disruption and insecurity in the hands of political actors, and how this relates to the type of security tied closely to political borders and 'states.' Because a link is established to the abstract notion of 'national security,' states are the actors called upon to re-establish control over the use of cybertechnologies through international norms, yet are also the actors mainly responsible for creating more insecurity.[18]

The role of the state in the literature

Computer scientists and engineers' reasons to study cybersecurity are driven by the aim to make technical systems more secure. The type of security that is sought is a combination of the three IT-security goals: integrity, availability, and confidentiality of a resource.[19] 'Cybersecurity governance' is the concept used to reach this type of security, a risk management approach based on continuous monitoring, measurement, and control of relevant processes.[20] The key concept here is 'regulation,' which comprises various governance tools, such as industry standards, national laws, or international agreements, with the prime aim being to establish 'trust' and stability of expectations among different actors.[21]

Technically-oriented cybersecurity research tends to focus little if at all on the role of the state, given its decidedly different focus. However, as soon as we move towards questions of information sharing and other organisational measures that are usually treated in the social science literature, the state makes an appearance in its multifaceted capacity as a governor. According to governance theory, *governance* becomes important when political power is highly fragmented. Fragmentation of political power can occur through decentralisation when government tasks and authority are delegated downwards (localisation), upwards (supranationalisation), or sideways (privatisation).[22] Fragmentation also takes place inside the government itself through ever-increasing functional differentiation of the administration.[23] Increasingly, performing tasks requires highly specific expert knowledge. The increasing division of labour, a hallmark of modern societies, blurs the lines between the public and the private sector. Many tasks that were previously performed by the state are now handled by specialised companies.

The network approach to governance therefore assumes that modern societies require new forms of public administration.[24] In this literature, the assumption is that the government can no longer simply issue instructions and monitor their implementation, but must also shape the framework conditions in such a way that cooperation operates smoothly even without constant oversight. Public administration thus becomes a team sport where persuasion, negotiation, and mutual trust are more important than control and regulation.[25] Thus, public services are provided by a plethora of independent, self-regulating, and self-organising networks. The role of the state in this type of literature is diverse. Depending on the research focus, the state and its bureaucratic entities is *security guarantor, legislator and regulator, or security partner*.

In the literature associated with international relations, there is a simpler view of the state. Predominantly, the use of cyberspace for strategic and military aims reinforces the neo-realist conception of interstate security in an anarchical system. In this system, states are 'black boxed' (they can all be treated as comparable units), and it is the balance of power which compels them to act in specific ways. Cyber offensive means are abstract instruments of power which can be used to threaten objects and services of value to the state and society (in peacetime and during conflict), and the question to be answered is whether they have a desired effect in a particular context. Given this conception, states are also the actors called upon to re-establish control over the misuse of cyberspace through international norms, often by looking to lessons from previous security issues and solutions, like nuclear deterrence or arms control. In their roles as *security guarantors*, states act to maximise power or security, or to minimise threats. When they are considered enemies by other states, state actors emerge as *threats*.

There is an additional role in the literature, mainly to be found in the literature that applies the Copenhagen School's securitisation theory to cybersecurity.[26] *Securitisation* signifies the sum of the representation of a fact, a person, or a development as a danger for the military, political, economic, ecological, and/or social security of a collective and the acceptance of this representation by the respective political addressee.[27] The successful securitisation of a topic justifies the use of all available means, including those outside the normal political rules of the game. Therefore, a strongly mobilising discursive justification for this extraordinary situation must be made in the political process. This happens above all in the narrative representation of great danger threatening the state or society.

Here, the role of the state and its bureaucracies is problematised rather than looked at instrumentally. Securitisation theory deals with a type of security that is discursively tied to the highest possible political stakes: the existential threats to the survival of the state and its society. The invocation of security sets in motion a securitisation process that has the power to lift the issue out of the 'normal' (desirable) political sphere, so that the associated threat can be dealt with swiftly and with all necessary means.[28] Measured against an ideal of 'normal politics,' security is suspect.[29] Hence, numerous scholars have foregrounded the normative implications of securitisation processes and called for opposing or reversing the process in order to return to 'normal politics' instead.[30] In this type of literature, the state and its representatives are *securitisers*, which, in certain contexts, can again amount to being a *threat* to other states and to society more broadly.

Historical Development of Cybersecurity Policy

In what ways does this view contrast with what we can learn from the evolution of the policy field? In this section, we will look at the 'evolutionary history' of cybersecurity into a political and security problem to show that 'the state' had (and has) different roles driven by various factors over the years. This creates the historical embedding of the discourse on which functions the state can, may, and wants to fulfil.

Telling the cybersecurity story from its inception means telling a strongly American-dominated story. Indeed, due to historical, political, social, and economic factors, the United States has shaped a large part of the information revolution in its early stages.[31] In particular—and importantly for the current debate about cybersecurity—the United States was at the forefront of developing specific ways of understanding both the benefits and the risks of the emerging information age.[32] When other countries began to think about the information age and politics, especially the needs of critical information infrastructure protection in the late 1990s, a lot of the policy concepts and threat perceptions were adopted from the United States, at least in their broad strokes. If we talk about the role of the state in what follows, we therefore claim some generalisability to other states, knowing that a detailed empirical analysis of different policies would unearth many country-specific details.[33]

More, better, more?

In the 1980s, the cyber threat was still regarded as primarily affecting government networks and the debate was fixed on cyber-espionage. Only in the later 1990s can a qualitative change in threat perception be observed. More and more (American) documents have made a connection between computers (or information infrastructures) and so-called critical infrastructures, with specific effects on the debate.[34] They are described as critical because a failure or substantial impairment of these organisations and institutions could have dramatic consequences for society. The implementation of all these infrastructures with IT is a rapidly progressing trend.

In the second half of the 2000s, two developments in cyber aggression began to emerge: the first (already mentioned) is a shift of focus away from theoretical 'doomsday' scenarios towards the reality of cyber aggression in conflict situations affecting both state and non-state actors. The reason for this shift is the 'normalisation' of cyber conflicts below the war threshold as a constant accompaniment to political conflicts. The second is more attention to targeted attacks. On the one hand, we have an increase in so-called 'mega hacks'—successful penetration into prominent economic or political targets. On the other hand, the focus of the political debate is now on so-called *Advanced Persistent Threats* (APTs)—capable actors, who use cyber means to achieve specific, persistent goals. Both mega hacks and APTs are a sign of the professionalisation of attackers and attacks, such as the Bundestag hack. Together, they refer to the increasingly direct and indirect roles that states play in cyber aggression.

But even though much has been reported about state-orchestrated cyber operations in the media in recent years, high-level attacks with considerable impact are still relatively rare. The exceptions confirm the rule: prominent examples are the attacks on Saudi Aramco in 2012, against the electricity network in Ukraine in 2015 and 2016, as well as the global infections by WannaCry and NotPetya in 2017. Cyber means were used mainly for disruptive actions and destabilisation of the political environment, but rarely for destruction, due to the difficulties of achieving clearly controllable effects, and due to the prevailing strategic restraint of states. More unspectacularly, the vast majority of cyber incidents that companies and individuals face on a daily basis do not make headlines. They are simply too banal to gain media attention.

The relative ordinariness of cyber life leads to the fact that the probability of an anticipated cyber catastrophe must be proven in the political process. For this to work, the risk of such an event's occurrence—always relying on anecdotes and events of the present as 'near misses' and to illustrate 'what could have been'—is presented as imminent. Following the logic of these mobilisation attempts, quasi-apocalyptic 'worst-case' scenarios are used, which are associated with a gigantic extent of damage. In combination, this means that the main threat is no longer the actual risk of the catastrophe, but rather non-action in the present. And last, but not least, the 'logical' reaction to this kind of danger representation is the reflex-like call, 'the state is not doing enough for cyber security!' But what can 'the state' do at all? In the following subchapters we look at solutions and problems.

Military perception of danger ...

Originally, there was a sensitisation to a new threat posed by the reorientation of security policy following the collapse of the Soviet Union, when the US began to focus more on non-state actors who could pose a threat to American citizens through terrorist attacks. It was significant and disturbing that the 'new opponent' could no longer be clearly identified. Consequently, uncertainty assessments increasingly assumed the potential danger of the means, which could be available to potential opponents of the US, as well as a focus on one's own vulnerabilities.

In the first half of the 1990s, US government documents began to contain a growing number of warnings that national security was increasingly threatened by possible cyberattacks on power plants, banks, air traffic control, or armed forces.[35] In the cybersecurity debate, hacking is seen not only as an activity that can be used by technically qualified individuals for minor offences, but also as a *modus operandi* for well-organised groups of actors with political intentions, such as terrorist organisations or states. Although most hackers may lack the motivation to use their knowledge to cause serious economic or social harm, government experts feared that people with these skills and low motivation could be made to act as cyber mercenaries incentivised by large sums of money.

Increasing warnings that national security is threatened by possible cyberattacks on critical facilities coincided with growing concerns about the vulnerability of US forces. Initially, the discussion about the *revolution in military affairs* and the computerisation of the armed forces was characterised by great euphoria. From the mid-1990s onwards, however, greater attention was also paid to possible risks. The formulation of strategies and doctrines, which no longer aim only at the enemy's forces, but also directly at their information flows, brought into focus the comparatively high vulnerability of the electronically strongly networked US troops. The further the discussion about attacks on the information systems of possible opponents progressed, the more intensively the possible dangers to one's own military and civil data networks were addressed.

... and civilian 'solution' approaches

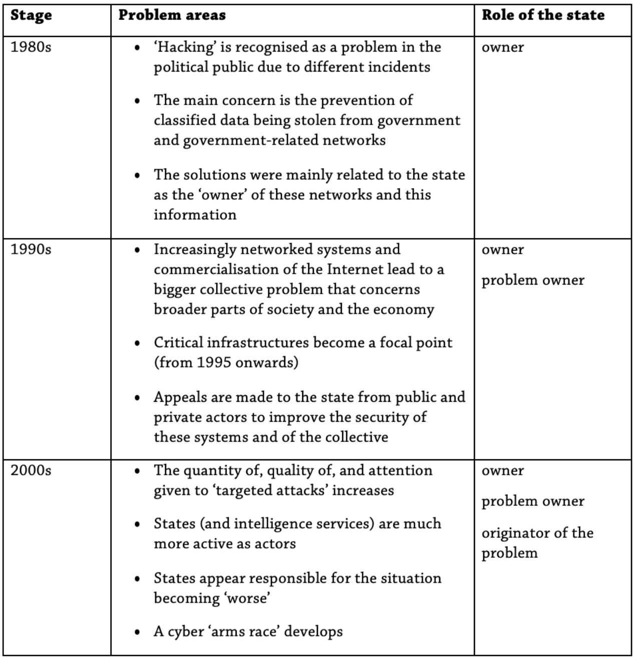
Due to the strongly military nature of the debate, the US Department of Defense's responsibility for threatening the critical information and communications infrastructure seemed clear. However, the difficulties in dealing with threats that were no longer territorially limited and could no longer be identified by any identifiable actors quickly raised fundamental questions about the division of competences and legal regulations, as well as political and technical strategies of a new security policy. There were difficulties in identifying the perpetrators (attribution). Assigning blame based on *cui bono* logic (stands for 'whose benefit?') alone, however, is not a legitimate basis for political or police action. In an attribution determination, the scenario of an operation under false flag (an operation in which a third party pretends to be another actor) must always be evaluated.[36] Uncertainties about the possibilities and limits of attribution help state actors credibly deny their existence, so that they can officially distance themselves from attacks at any time.[37]

While the doctrine for information warfare was further developed in the military area,[38] in the civilian area other actors tried to get a grip on the vulnerability of society as a whole due to its dependence on inherently insecure information infrastructures. In 1995, the US *Presidential Commission on Critical Infrastructure Protection* (PCCIP) was established to produce a comprehensive report on the security of all US infrastructure systems. The main focus was on the still largely unknown threats from cyberspace. The PCCIP should assess these risks, develop defensive measures, and contribute to clarifying the institutional and legal reform needed. *All* relevant agencies were represented in the Commission, no longer just the security policy apparatus. In addition, the private infrastructure owners were also included. This approach assumed that, in the case of critical infrastructure protection, security policy could no longer be an exclusive task of the state, but required a sharing of responsibility, in particular, with the private sector.[39] The final report of the PCCIP laid the foundations for the ways in which critical infrastructures and critical information infrastructures are protected worldwide today.[40]

Thanks in part to the revelations by former US National Security Agency employee Edward Snowden, we now know that intelligence services are probably the most important players when it comes to the strategic use of cyberspace. Precisely because of the focus on spectacular 'cyber war' scenarios, which could clearly be situated in the area of military operations, research has long overlooked how the practices in this community shaped strategic behavioural norms in cyberspace over many years. It is particularly important for the following explanations that intelligence services exploit (non-public) security gaps in common operating systems to exploit numerous strategically opportune locations of the Internet infrastructure for various purposes. Their accesses and implants can be used for numerous purposes (surveillance, espionage, disruptive actions, etc.) and can theoretically be activated at any time if they remain unknown to the victim. Such infected machines reduce the security of the entire system, and there is no guarantee that these gaps will not be detected and exploited by another party, such as other intelligence agencies, criminal hackers, or other politically motivated actors. The security of the entire Internet is thus deliberately—or for strategic reasons—endangered. Thus, the paradoxical situation arises that state actors are directly responsible for indirectly endangering the very same national security for which they are responsible.[41]

Role of the State in Cybersecurity Policy

Historically, we see a development of the roles of the state coinciding with three phases in cybersecurity policy. In a first role, the state appears as the owner of endangered networks *(owner)*. In a second role, the state appears as the actor who must solve the problem in terms of security policy *(problem owner)*. Third and finally, the state or individual units within the state appear as the originator of the problem *(originator of the problem)*. Importantly, this development is additive: new roles are assumed, whilst old ones remain, thereby increasing the complexity of the cybersecurity policy field. This development is shown schematically in Table 1.



Stage	**Problem areas**	**Role of the state**
1980s	• 'Hacking' is recognised as a problem in the political public due to different incidents • The main concern is the prevention of classified data being stolen from government and government-related networks • The solutions were mainly related to the state as the 'owner' of these networks and this information	owner
1990s	• Increasingly networked systems and commercialisation of the Internet lead to a bigger collective problem that concerns broader parts of society and the economy • Critical infrastructures become a focal point (from 1995 onwards) • Appeals are made to the state from public and private actors to improve the security of these systems and of the collective	owner problem owner
2000s	• The quantity of, quality of, and attention given to 'targeted attacks' increases • States (and intelligence services) are much more active as actors • States appear responsible for the situation becoming 'worse' • A cyber 'arms race' develops	owner problem owner originator of the problem

Table 1. Historical Roles of the State

As we saw in the previous section, the literature in international affairs focuses most strongly on the third and most recent role. However, cybersecurity policy documents from a variety of states display a much bigger empirical diversity.[42] Through these, cybersecurity reveals itself as a typical cross-cutting issue, which requires cooperation between a wide variety of actors. Actors are not only drawn from a variety of public authorities, but also from business and civil society.

It is a truism that the state alone cannot ensure an increase of cybersecurity, not least because many crucial networks are in private hands. Cybersecurity is also to a large extent the responsibility of every individual and every company. Not only is industry (also including small and medium-sized enterprises) particularly affected by cybercrime and espionage; most critical infrastructures are also privately owned, so the state cannot guarantee their protection against cyberattacks. In addition, the broad range of necessary countermeasures includes many elements that cannot be designed or implemented by the state alone.

A rundown of all the roles given to the state reveals the following. First, the state is to secure its own civil and military networks against all forms of cyber conflict by technical and other means. In this role, the state acts as *guarantor and protector* of the central state institutions.

The state has other roles in its function as *legislator and regulator.* On the one hand, it creates the necessary legal basis to clarify its hierarchical function vis-à-vis society and the economy. It does this, for example, in the fight against cyber crime or in the regulation of critical infrastructures (those whose disruption could seriously harm society). On the other hand, it also creates the legal framework to regulate the tension between citizens and businesses. This happens, among other things, with safety regulations in product certifications, or in the legislation on manufacturers' liability for products with digital components. How and to what extent this role is exercised varies and depends on the historically developed relationship between the economy and the state.[43]

Since actors in cyberspace often operate internationally, the international dimension, especially around criminal law cooperation, is also of great importance. State institutions act as *supporters/representatives of society* by advocating for international frameworks that are conducive to both the respective economy and civil society.

In addition to its role as a regulator, in the field of critical infrastructures the state also plays the *role of a partner*. Many Western countries are trying to provide more protection through so-called public-private partnerships. Most of these take place in voluntary cooperation between industry and the state, particularly in the area of information exchange. The partnerships are based on the insight that, apart from a complete nationalisation or a completely private security architecture of critical infrastructures, national security issues in the cybersecurity area can only be addressed jointly.

Raising awareness on cyber issues among the general public is also a major policy endeavour. The state often plays the role of a *knowledge creator and disseminator*, in which it wants to be perceived as a trustworthy source of information. Whether or not this will succeed depends on the relationship of trust that has developed historically between different groups in society and state institutions, in some cases in very different ways. In this function, the state acts as a *securitiser* by using its position of trust to disseminate a certain representation of danger.

The relationship of trust is also an important component of *the role of the state as the originator of more cyber-in-security*. The state, in the context of its intelligence activities, also acts as a threat to some; this dimension is not new, but it is particularly accentuated through the rapid technical advancement witnessed over the past ten years. Domestically, this can be the case, for example, in the defence against terrorism and espionage, but also in the prevention of violent political extremism. In some societies, a history of the misuse of these competences for unjustified state interference in civil rights reinforces the perception of the state as a danger. In addition, political and economic espionage emanating from foreign states reinforces the perception of states as sources of danger. In this role, state action is thus declared a problem; the state becomes the originator of the problem—it becomes the *securitised*.[44]

Three Areas of Tension Between the State, Economy, and Society

A satisfactory level of cybersecurity can only be achieved by government, business, and society together. However, the subgroups within these sectors often have different interests. This gives rise to at least three areas of tension in which every cybersecurity policy should be consciously positioned. Where cybersecurity policy is prescribed on these axes and where it moves to is the result of complex negotiation processes that are strongly dependent on individual events and related perceptions of danger (see Figure 1).

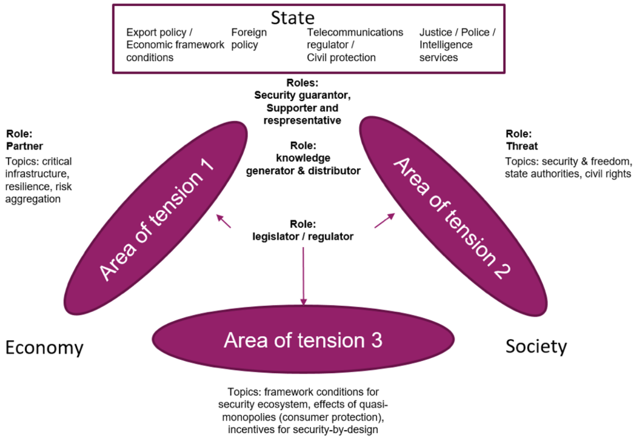

State
Export policy / Economic framework conditions
Foreign policy
Telecommunications regulator / Civil protection
Justice / Police / Intelligence services
Roles: Security guarantor, Supporter and respresentative
Role: knowledge generator & distributor
Role: legislator / regulator
Role: Partner
Topics: critical infrastructure, resilience, risk aggregation
Role: Threat
Topics: security & freedom, state authorities, civil rights
Area of tension 1
Area of tension 2
Area of tension 3
Economy
Society
Topics: framework conditions for security ecosystem, effects of quasi-monopolies (consumer protection), incentives for security-by-design

Figure 1. The three areas of tension in cybersecurity policy (own graphic)

In the first area of tension between the state and the economy, it is necessary to formulate a policy for securing critical infrastructures that absorb the negative consequences of liberalisation, privatisation, and globalisation from the point of view of security policy without preventing their positive effects. In this area of tension, the state is concerned with the dependence on economic action and the resulting resilience of society. How can trust be created between business and government? Where must the state intervene in order to prevent risk aggregations and contagion effects that pose a threat to society? Finding answers to these questions takes place in this area of tension and is an important part of the cybersecurity policy process.

In the second area of tension between the state and citizen, it is necessary to find the politically desired balance between more security and more freedom in the digital space. Additional police or intelligence powers often come into conflict with civil rights: specifically, the basic right to informational self-determination or anonymity on the Internet. When cyberthreats are discussed in depth, people tend to forget that, despite increased attention and calls for more and better protection, cybersecurity is just one of many complex intersectoral issues that the state has to address today. The harm caused by past cyber incidents may not be high enough (or may not be experienced as directly) to make substantially higher costs and cuts in civil rights acceptable. Rather, the harm perceived in other issues (such as terrorism) serves as legitimisation to make cuts in the political discourse in cybersecurity issues (e.g., the encryption policy debate).

In the third area of conflict between citizens and business, it is necessary to set the framework conditions for the development of a successful security ecosystem. How can the market, which is also confronted with the problem of quasi-monopolies, be regulated in such a way that an optimal balance between safety and functionality is achieved? How can incentives for more safety obligations be created for service providers? How can users be sensitised to the fact that they no longer put more functionality before thinking about safety? How can the (global) legal framework conditions for activities in virtual space be harmonised to counteract the danger of loopholes and the priority of cheap solutions?

What is taken for granted by economic and civil society actors also applies to the roles of the state: it assumes a multitude of roles. It is therefore not surprising that in many cybersecurity policy issues, the state represents a wide variety of interests at the same time. Consequently, thematic alliances are formed between different departments of the state with different interest groups of the economy and society. Each of these different political groups represents a different vision of the role of the state in the issue at hand.

In democracies, such role conflicts are dealt with at the political level and can be approached systematically. For example, while the state has, for the purpose of an effective criminal prosecution and modern intelligence capabilities, an interest in the use of vulnerabilities for surveillance, it also has an interest in the greatest possible use of secure technologies and their use by business and society. In some states, this conflict of objectives is managed politically in an institutionalised vulnerability management process. Among other things, the public interest in secure platforms is contrasted with the public interest in the effectiveness of law enforcement. The recognition of the legitimacy of the multiple roles of the state helps to structure this consideration in an institutionally meaningful way and to recognise that decisions in this area take on an intrinsic political dimension.

Conclusion

In this article, we have explained the main features of cybersecurity policy through an investigation of its depiction in the literature and an analysis of policy documents. Our analysis shows that cybersecurity policy is diverse and necessarily includes state, economic, and societal actors. The variety of different countries in the historically evolved constellations of state, economy, and society determine the possibilities and limits of state roles, and political conflict about these roles.

The recognition of the diversity of government action is a solid foundation for developing strategic options, which then can lead to an overall strategy. An overall strategy for cybersecurity policy should create clear relationships as to how the various goals are weighed against each other, and should clearly identify the goal the state fulfils in its various roles. From a strategic point of view, role conflicts can be analysed in advance and included in political processes. This enables basic strategic decisions to be made (e.g., in the area of offensive powers of private actors), but also a strategic management of role conflicts (e.g., in the area of vulnerability management).

Even if the results look dissimilar in different countries, the areas of tension in which cybersecurity policy takes place remain the same. Cybersecurity policy revolves mainly around defining the various roles of the state in cybersecurity (and through so doing also those of semi- and non-state actors).[45] It should be noted that such clarifications, in a rapidly changing technological and political environment, are always temporary and subject to political scrutiny and shifts of power. Changing social and political coalitions are reflected in new political decisions, which are discernible in several generations of cybersecurity strategies.

While the topics of political interaction are similar in different countries, the concrete manifestation of different roles depends on the strength of the different interest groups and the historically evolved distribution of roles and relationships of trust between the actors. Topics include questions of the limits of responsibility (i.e., where does the responsibility of the state, the economic, and societal actors begin and end?) and questions of the concrete assumption of this responsibility (i.e., which means may which actor use to fulfil their role?). As shown in this article, the answers to both questions are the results of multi-faceted political cybersecurity processes. As a structuring element, we have proposed that the political debates be divided into three areas of tension and six roles. This enables a more systematic analysis of political conflicts in the field of cybersecurity.

*Acknowledgments: The authors thank Jasper Frei for his excellent research assistance for this article

Notes

[1] Robert S. Dewar, ed., "National Cybersecurity and Cyberdefense Policy Snapshots," Center for Security Studies (CSS) Collection 1 (2018), ETH Zurich, accessed February 5, 2019, https://www.research-collection.ethz.ch/handle/20.500.11850/314596.

[2] The use of the "black box" term "state" is chosen deliberately, as this corresponds to the usage of language in international relations. See Sean Fleming, "Artificial Persons and Attributed Actions: How to Interpret Action-Sentences About States," European Journal of International Relations 23, no. 4 (2017): 930-50.

[3] See, for example, the deterioration of relations between Russia and the West and the associated increase in cyber activities between the two: [Marie Baezner and Patrice Robin, "Cyber-conflict between the United States of America and Russia," CSS Cyber Defence Hotspot Analysis 2 (2017): 1-28.]

[4] Cyberspace is understood here as the totality of all computers and network components (including the entire Internet, but also separate networks) and associated content. See Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security 38, no. 2 (2013): 17.

[5] Robert S. Dewar, "The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern," in Challenges and Critiques of the EU Internal Security Strategy, ed. Maria O'Neill and Ken Swinton

(Newcastle upon Tyne: Cambridge Scholars Publishing, 2017), 113-48.

[6] The reports are available on the website of the Center for Security Studies, ETH Zürich, "Risk and Resilience Reports": http://www.css.ethz.ch/en/publications/risk-and-resilience-reports.html.

[7] The conceptualisation of this article concerns only liberal democracies, since this political model enables different, contested roles of the state, and makes the debate about it possible in the first place.

[8] Rossouw von Solms and Johan van Niekerk, "From information security to cyber security," Computers & Security 38 (2013): 97–102.

[9] Important: Because the content in the databases is expanded constantly, the findings have to be taken with a grain of salt, or rather, with some scepticism. However, we believe that the numbers and observations can serve as indicators of trends. On the technicalities: searches were done for 'cybersecurity' OR 'cyber-security' OR 'cyber security' because the databases distinguish between the different spellings. For better comparability, searches were done for 'article title, abstract, and keywords' (rather than 'all fields') in Scopus, to match the category 'topic' in WoS, which contains title, abstract, and keywords. Searches in WoS were done in All Databases and not only in the Web of Science™ Core Collection. In general, the high competition between the two providers leads to improvements in the services offered, and therefore, to frequent changes in the database content. For example, Scopus has actively tried to reduce the negative bias towards the Social Sciences and the Arts and Humanities through the inclusion of more books in the last few years. Also, both databases have continually increased their coverage of non-English language content. See Philippe Mongeon and Adèle Paul-Hus, "The journal coverage of Web of Science and Scopus: a comparative analysis," Scientometrics, 106(1) (2016): 213-228; Jie Li, Judie F. Burnham, Trey Lemley and Robert M. Britton, "Analysis: Comparison of Web of Science, Scopus, SciFinder, and Google Scholar," Journal of Electronic Resources in Medical Libraries 7, no. 3 (2010): 196-217.

[10] The ranking of articles in both databases is done via citation-count.

[11] Multiple categories per entry are allowed.

[12] The top-cited paper in both databases in this category is Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," Information Systems Research 16, no. 2 (2005): 186-208.

[13] Cf. Iván Arce, "The Weakest Link Revisited," IEEE Security & Privacy 1, no. 2 (2003): 72-76.

[14] Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," International Journal of Critical Infrastructure Protection 2(4) 2009: 179-187; also Dan Assaf, "Models of Critical Information Infrastructure Protection," International Journal of Critical Infrastructure Protection 1 (2008): 6-14.

[15] Exemplary: Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35, no. 1 (2012): 5-32; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," Journal of Information Technology & Politics, 10, no. 1 (2013): 86-103.

[16] Adam P. Liff, “Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War,” Journal of Strategic Studies 35, no. 3 (2012): 401-428.

[17] Exemplary: Brandon Valeriano and Ryan C. Maness, “The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11,” Journal of Peace Research 51, no. 3 (2014): 347–60.

[18] For a historical overview see: Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013); Michael Warner, “Cybersecurity: A Pre-history,” Intelligence and National Security 27, no. 5 (2012):781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.

[19] Exemplary: Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed, (Indianapolis, IN: Wiley, 2008).

[20] Pauline Bowen, Joan Hash, and Mark Wilson, Special Publication 800-100 Information Security Handbook: A Guide for Managers (Gaithersburg: National Institute of Standards and Technology (NIST), 2006), 6.

[21] Laurin B. Weissinger, Modelling Trust and Trust-Building among IT-Security Professionals: How do practitioners find out whom to work with? Lecture Notes in Computer Science, 10292 (2017), 557–566.

[22] Elke Krahmann, “Conceptualizing Security Governance,” Cooperation and Conflict 38 (2003): 6–26.

[23] Mark Bevir and R.A.W. Rhodes, A Decentered Theory of Governance: Rational Choice, Institutionalism, and Interpretation, Working Papers of the Institute of Governmental Studies, Number 10, (Berkeley, 2001).

[24] Guy Peters and John Pierre, “Governance Without Government? Rethinking Public Administration,” Journal of Public Administration Research and Theory 18 (1998): 223–43.

[25] Lester M. Salamon, “The Tools Approach and the New Governance: Conclusion and Implications,” in The Tools of Government: A Guide to the New Governance, ed. Lester M. Salamon (Oxford: Oxford University Press, 2002), 600–10.

[26] Johan Eriksson, Cyberplagues, “IT, and Security: Threat Politics in the Information Age,” Journal of Contingencies and Crisis Management 9, no. 4 (2001): 211-22; Dunn Cavelty, U.S. Efforts; Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber-Security, and the Copenhagen School,” International Studies Quarterly 53, no. 4 (2009): 1155-75; Sean Lawson, “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats,” Journal of Information Technology & Politics 10, no. 1 (2013): 86-103. Also, with focus on metaphors, David Barnard-Wills and Debi Ashenden, “Securing Virtual Space: Cyber War, Cyber Terror, and Risk,” Space and Culture 15, no. 2 (2012): 110-23; David J. Betz and Tim Stevens, “Analogical Reasoning and Cybersecurity,” Security Dialogue 44, no. 2 (2013): 147-64; Myriam Dunn Cavelty, “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse,” International Studies Review 15, no. 1 (2013): 105-22.

[27] Barry Buzan, Ole Waever, and Jaap De Wilde, Security: A New Framework for

Analysis (Boulder, CO: Lynne Rienner, 1998).

[28] Ole Wæver, "Securitization and Desecuritization," in On Security, ed. Ronnie D. Lipschutz (New York/Chichester: Columbia University Press, 1995): 46-86; Jef Huysmans, "The Jargon of Exception - On Schmitt, Agamben and the Absence of Political Society," International Political Sociology 2, no. 2, (2008): 165-83; Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder: Rienner, 1998).

[29] Lene Hansen, "Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it," Review of International Studies 38, no. 3 (2012): 525-46; 528.

[30] See for example Claudia Aradau, "Security and the democratic scene: Desecuritization and emancipitation," Journal of International Relations and Development 7, no. 4 (2004): 388-413; Hansen, "Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it"; Jef Huysmans, "The Question of the Limit: Desecuritisation and the Aesthetics of Horror in Political Realism," Millennium - Journal of International Studies 27, no. 3 (1998): 569-89; Philippe Bourbeau and Juha A. Vuori, "Security, Resilience and Desecuritization: Multidirectional Moves and Dynamics," Critical Studies on Security 3, no. 3, (2015): 253-68.

[31] On the particular U.S. development, see Dunn Cavelty, U.S. Efforts; Jason Healey, A fierce domain: conflict in cyberspace, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013); Michael Warner, "Cybersecurity: A Pre-history," Intelligence and National Security 27 (5) (2012): 781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.

[32] Dunn Cavelty, U.S. Efforts.

[33] Myriam Dunn Cavelty, Cybersecurity in Switzerland, Springer Briefs in Cybersecurity. (Cham: Springer International Publishing, 2014).

[34] Dunn Cavelty, U.S. Efforts.

[35] Ralf Bendrath, "Elektronisches Pearl Harbor Oder Computerkriminalität? Die Reformulierung Der Sicherheitspolitik in Zeiten Globaler Datennetze," Sicherheit und Frieden (S+F) / Security and Peace 18, no. 2 (2000): 135-44; Michael Warner, "Cybersecurity: A Pre-history," Intelligence and National Security 27, no. 5 (2012):781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.

[36] Timo Steffens, Auf Der Spur Der Hacker: Wie Man Die Täter Hinter Der Computer-Spionage Enttarnt (Berlin: Springer Vieweg, 2018), 127-137 (On The Trail of the Hackers: How to Expose Offenders Behind Computer Espionage). For more on attribution, see Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38, no.1-2 (2015): 4-37.

[37] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," International Political Sociology 4, no.1 (2010): 12, 15-32, Even though such distancing is not always plausible, see Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," International Affairs 94, no. 3 (2018): 477–494.

[38] Myriam Dunn Cavelty, "Cyberwar," in The Ashgate Research Companion to Modern Warfare, ed. George Kassimeris and John Buckley (Ashgate, 2010), 123-

144.

39 Dunn Cavelty and Suter, Silver Bullet, 179-87.

40 President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (Washington, 1997). Accessed May 17, 2019. https://www.documentcloud.org/documents/2800106-Document-02-President-s-Commission-on-Critical.html

41 For the strategic impetus that drives this behaviour, see Ben Buchanan, The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations (Oxford: Oxford University Press, 2017).

42 Dewar, National Cybersecurity and Cyberdefense Policy Snapshots.

43 Peter A. Hall and David Soskice, Varieties of Capitalism: The Institutional Foundations of Comparative Advantage (Oxford: Oxford University Press, 2001).

44 Developing this view and beyond, see Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," Ethics & International Affairs 32, no. 4 (2018): 411-24, accessed April 2, 2019, doi: 10.1017/S0892679418000618.

45 Florian J. Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates" (PhD diss., University of Oxford, 2018).