UNIVERSITY OF COPENHAGEN
FACULTY OF SOCIAL SCIENCES

EU Cybersecurity Governance

Redefining the Role of the Internal Market

PHD DISSERTATION 2019

Tobias Liebetrau

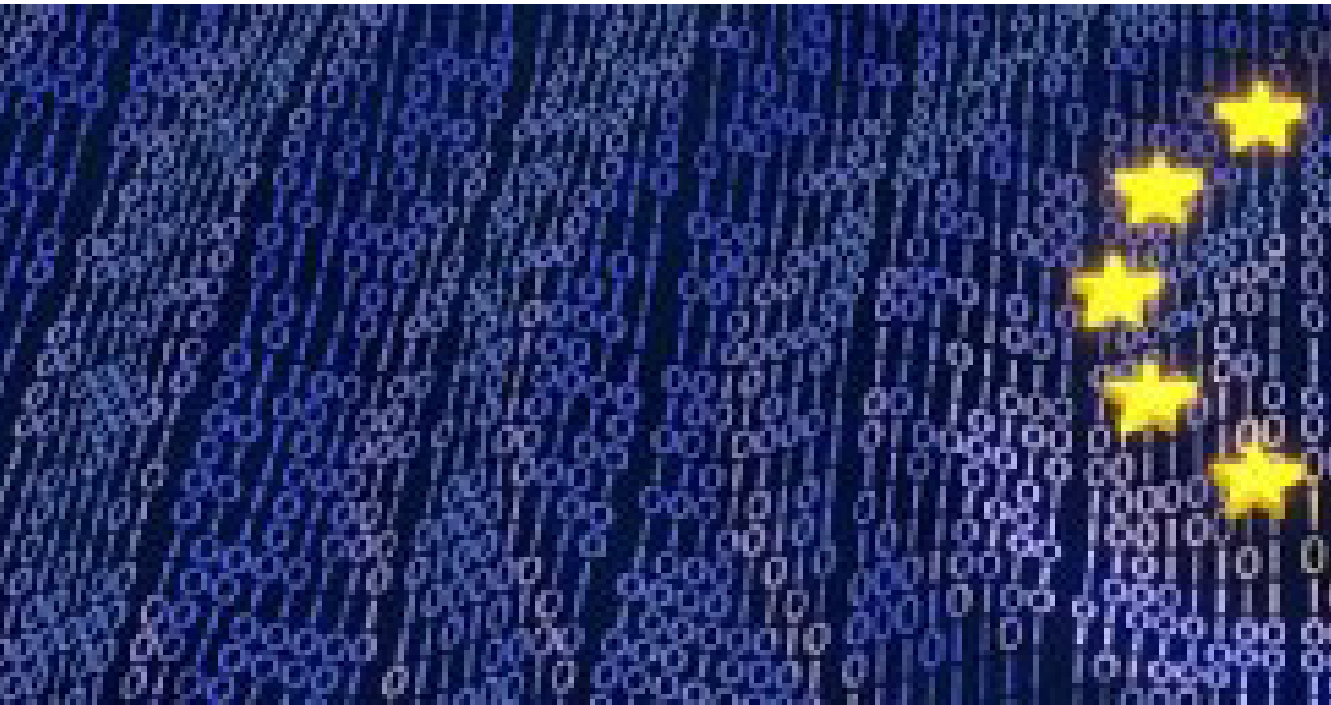
DEPARTMENT OF POLITICAL SCIENCE
FACULTY OF SOCIAL SCIENCES
UNIVERSITY OF COPENHAGEN · DENMARK
PHD DISSERTATION 2019 · ISBN 978-87-7209-274-4

TOBIAS LIEBETRAU

EU Cybersecurity Governance

Redefining the Role of the Internal Market

SL grafik



EU Cybersecurity Governance

Redefining the Role of the Internal Market

PhD dissertation

Tobias Liebetrau

PhD dissertation submitted at the Department of Political Science, University of Copenhagen

Supervisor: Karen Lund Petersen

Data of submission: 8 March 2019

Data of public Defence: 20 June 2019

Assessment Committee:

Professor Ben Rosamond, University of Copenhagen (chair)

Senior Lecturer Andrew Neal, University of Edinburg

Senior Lecturer, Myriam Dunn Cavelty, ETH Zürich

ISBN 978-87-7209-274-4 (Printed book)
ISBN 978-87-7209-282-9 (E-book)
Printed by SL grafik, Frederiksberg, Denmark (slgrafik.dk)

Table of contents

Tables and figures

Acknowledgements

Abandoning the Danish Defence Intelligence Service's chamber of secrets to pursue a PhD at the ivory tower of KU turned out to be much a much less isolated and lonely endeavour than I feared. Science is, indeed, social. That I have succeeded in arriving at a completed PhD dissertation, I owe, largely to the many people that have supported and helped me along the way. I would like to thank a few of them here.

First, I wish thank my family for their constant support and patience, expressions of love and determination to combine hard work with joie de vivre. On that note, I would like to thank my friends for constantly reminding me that there are more important things in life than research and career. The combined efforts of 'Gruppen med alle', 'Pippoismen', LiebeVin (including our loyal customers) and many others helped to make sure I never lost my soif de vivre.

My supervisor Karen Lund Petersen deserves special thanks. She kept encouraging me to apply for a PhD position despite one failed attempt, inspired me to write the dissertation on this topic and took time out of her demanding schedule for in-depth conservations and contemplations. I would also like to thank the Department of Political Science and the Head of the PhD School Christian Rostbøll for accepting me to the program. In addition, I'm grateful for the support and hosting offered by Professor Didier Bigo and everyone at Le Centre de Recherches Internationales (CERI), Sciences Po Paris, in the first half of 2017.

Friends, peers and colleagues have provided valuable input and feedback throughout the process. Special thanks goes to Kristoffer Kjærgaard Christensen, the first half of the 'Cyber Squad', for countless hours of talking, reading and writing. Without our collaboration, this journey would have been much less thought provoking and fun. I would also like to thank Manni Crone and Olaf Corry who took time to read and provide extremely helpful comments on the first draft of the entire dissertation. For their feedback and input for different parts of this dissertation I am also grateful to,

among others, Christopher Gad, Jens Erik-Mai, Trine Villumsen Berling, J. Peter Burges, Lene Hansen, Anders Wivel, Ole Wæver, Peter Marcus Christensen and everyone else at CAST and in the IR group at the Department of Political Science.

I also want to express my gratitude to PhD group at the department who, in addition to deliver collegial support and invaluable comments, helped to make sure that PhD life turned out fantastic. My special thanks go to, Irina, Jessica, Anne, Anne, Alexei, Morten, Niels, Rune, Christine, Kitt, Isabel, Lasse, Simone, Wiebke, Troels, Agnete, Jonas, Hjalte, Anine, Livia, Benjamin, Yev, Malte, Anders and Dean.

Last, but not least, I owe a big thank you to the interviewees and all the people who engaged with my research in the past years at conferences, workshops, hearings, dinners etc.

Tobias Liebetrau

Copenhagen, March 2019

I. Digitization, Marketization and European Security Governance

> 'Europe is still not well equipped when it comes to cyber-attacks. Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. Last year alone there were more than 4,000 ransomware attacks per day and 80% of European companies experienced at least one cyber-security incident. Cyber-attacks know no borders and no one is immune.' (Juncker 2017)

This is how the head of the EU Commission, Jean-Claude Juncker, in his State of the Union Speech 2017 described the cyber threat facing the European society. In the speech, Juncker made better protection of Europeans in the digital age a top priority in the year to come and he emphasized the need for additional EU effort in the field of cybersecurity. Juncker's remark is particularly telling for two reasons. First, when cybersecurity threats are framed as knowing 'no borders and no one is immune' conventional spatial and functional modalities of European security governance are put to question. Second, when cyber-attacks are framed as an existential threat that are 'more dangerous to the stability of democracies and economies than guns and tanks' it potentially opens a space for and further legitimizes EU action in the field of European security governance. Juncker's statement raises challenging questions regarding what is to be secured, by who and how. As such, it speaks to the distribution of European security governance authority and responsibility in the contemporary digital age.

The link between digital technologies and security is often presented as following naturally from the inevitable development and implementation of these same technologies. It has become an indisputable and obvious truth that cybersecurity prevails on today's security political agendas and in the military budgets all over the world. However, the link between digital technologies, cyberspace and security is not given. It has been brought into being in political and technocratic processes at various empirical

sites. This dissertation, on the one hand, seeks to account for the emergence and development whereby the digitization of the European societies and the pervasiveness of information and communication technologies (ICT) acquired the politically salient status of being an EU security issue, and it seeks to understand the implications of it on European security governance modalities, on the other hand.

Besides being framed as a security issue, the digitization of society speaks to economic growth and social transformation. The past decades people all over the world have cracked their brains on how to reap the economical and societal fruits of the digital revolution. The myriad of opportunities on the digital horizon seem endless. European Union policy is no exception from this trend and the digitization of the European societies has been a key driver in European integration since the 1980's. So far, it culminated in 2015 with the EU presenting its strategy on the prominent Digital Single Market. The strategy underlines that digitisation and ICT have become the foundation of the economy and transforms our lives and societies:

> 'The global economy is rapidly becoming digital. Information and Communications Technology (ICT) is no longer a specific sector but the foundation of all modern innovative economic systems. The Internet and digital technologies are transforming the lives we lead, the way we work – as individuals, in business, and in our communities as they become more integrated across all sectors of our economy and society.' (European Commission 2015: 3)

In short, the digitization of the European society is framed as inescapable and ICT as ubiquitous. At the same time, the increasing digitization of the European society continues to promise prosperity and economic growth. It is, however, an inherent dilemma to be solved that the perhaps most promising economic feature in contemporary political life – increased digitization and technological development – is now also considered one of the biggest security threats to our societies and ways of living. Digitization is a Janus-faced phenomenon in which every piece of new digital technology is invariably

accompanied by uncertainties and vulnerabilities (inherent to e.g. a piece of software itself as well as the many unforeseen and future ways it can be put to use) which have to be governed and managed. Although the development of digital technologies have opened up many promising prospects in terms of economy, welfare, health etc., it has also produced a large number of daunting security political and democratic debates that remain unresolved.

Tech-intensive societies hence face a paradoxical and seemingly endless multiplication of socio-technically manufactured uncertainties, which forces us to think anew about the relationship between technology, politics, security and private companies. As the dissertation will demonstrate, the changing conditions of possibility emerging from the dynamics of contemporary digital technological development give rise to new forms of European security governance. These new forms of European security governance call into question longstanding political categories and demarcations such as public-private, market-military, national-European and technological-political. Moreover, the changing conditions of possibility for European security governance question the conventional distribution of security governance authority and responsibility.

Given the centrality of digitization, it is not surprising that the EU is gradually getting more involved in cybersecurity governance (See e.g. Christou 2016; Barrinha and Carrapico 2017). The EU Commission in May 2017, under the Digital Single Market Strategy midterm review, identified the tackling of cybersecurity threats as one of its three key priority areas for further EU action in the years to come (European Commission 2017). Likewise, on 13 September 2017, the same day as Juncker's State of the Union Address, the EU Commission adopted a cybersecurity package with new initiatives to further improve EU cyber resilience, deterrence and defence efforts. The 2017 EU Commission cybersecurity package, had been preceded by the first ever EU cybersecurity strategy in 2013. The 2013 EU cybersecurity strategy paved the way for achieving progress at political, legislative and capability level. What the political dimension is concerned, cybersecurity is now among one of the

EU's most important priorities, with cybersecurity elements having been integrated transversally within other EU policies, including the prominent Digital Single Market project (European Commission 2015). In 2016, the EU adopted the first ever legislation on cybersecurity – the Network and Information Security Directive (NIS). In terms of capabilities, both the European Network and Information Security Agency (ENISA) and the European Cyber Crime Center (EC3) experienced a boost in the period from 2013 to 2017.

In sum, the development leaves no doubt that the European societies increasing digitization has become pivotal to both Internal Market and EU security governance development and integration. To an extent, I argue, that it is crucial to account for the development whereby the increased digitization of European societies has become an EU security issue, how this apparent EU Internal Market-security nexus plays out and to assess its political consequences. What is under investigation in this dissertation, then, can be boiled down to two research questions:

> *How did EU cybersecurity governance emerge and develop? To what implications for European security governance?*

The argument in a nutshell

Since World War II security has primarily been associated with national security, necessity and raison d'état (Wæver 2003). Security, it is traditionally said, cannot be compromised (Baldwin 1997; Walt 1991; Wolfers 1952). The EU is built on the same logic. Originally, the transnational organization of European markets and industries was considered a means to secure peace following World War II. This prescribed a clear division of labor, responsibility and authority. Security was a prerogative of the member states, while the European community should foster market integration and interdependencies. Article 4(2) of the Treaty of the European Union clearly states that national security is a member state privilege: