Council of the European Union
General Secretariat

READING REFERENCES
Council Library

2019

CYBER SECURITY LAW AND POLICY

© Viivi Myllylä, Prime Minister's Office, Finland

Council of the European Union
Rue de la Loi/Wetstraat 175 - B-1048 Bruxelles/Brussel - Belgique/België
Tel. +32 (0)2 281 65 25
Follow us http://www.consilium.europa.eu/en/library-blog/ - #EUCOlibrary

Introduction

Cyber law and cyber policy are becoming crucial topics. In April 2019, the Council adopted the EU Cybersecurity Act. Following month, the Council established frameworks that allows the EU to impose sanctions towards persons or entities that are "responsible for cyber-attacks or attempted cyber-attacks, provide financial, technical or material support for such attacks, or are involved in other ways".

With October being the European Cyber Security month, as well the Finnish Presidency's priority on hybrid and cyber threats, the Council Library has compiled a reading list focusing on cyber law, security, and policy. It contains numerous books and articles that you can access via Eureka.

Resources selected by the Council Libraries

Please note:

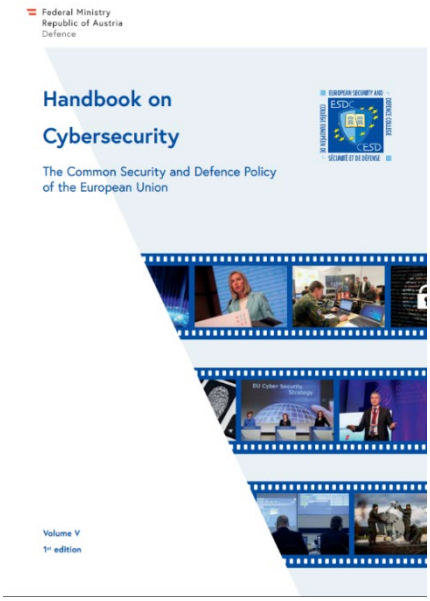
This bibliography is not exhaustive; it provides a selection of resources made by the Council Library. Most of the titles are hyperlinked to Eureka, the resource discovery service of the Council Library, where you can find additional materials on the subject. Access to some resources might be limited to registered Council Library users or to users in subscribing institutions.

The contents are the sole responsibility of their authors. Resources linked from this bibliography do not necessarily represent the positions, policies, or opinions of the Council of the European Union or the European Council.

Reuse of the covers is prohibited, they belong to the respective copyrightholders.

Additional resources may be added to this list by request - please contact the Council Library to suggest a title: library@consilium.europa.eu

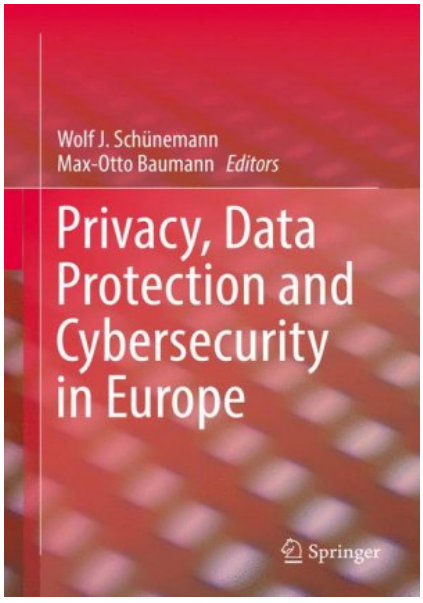
Books



Handbook on cyber security

Jochen Rehrl; European Security and Defence College ; Federal Ministry of Defence of the Republic of Austria
Luxembourg : Publications Office, 2018
Access via Eureka

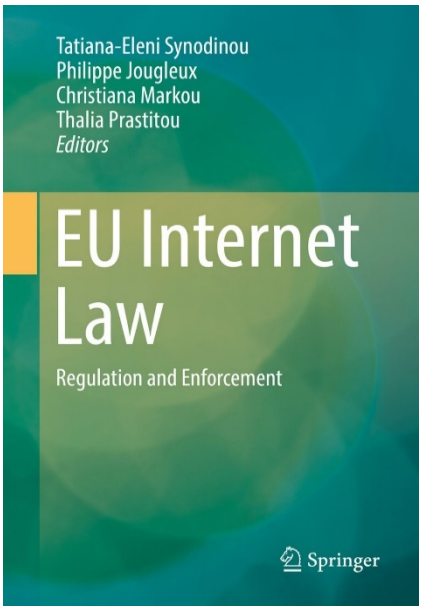
"The present handbook gives an overview of the state of affairs in European cybersecurity. It was edited and published by the Ministry of Defence of Austria during the Austrian Presidency of the Council of the European Union. It is the fifth handbook in the series of CSDP publications. In a global context where security is never just a matter of traditional defence and where the real world merges with the cyberworld, cybersecurity is a collective responsibility. It calls on each and every one of us, citizens of Europe, to invest in the most powerful tool we have to exercise our sovereignty, advance our interests and stand by our values: our European Union."



Privacy, data protection and cybersecurity in Europe

Wolf J Schünemann ; Max-Otto Baumann
Cham : Springer, 2017
Available at Legal Library Main Collection (SJUR INF 104632)

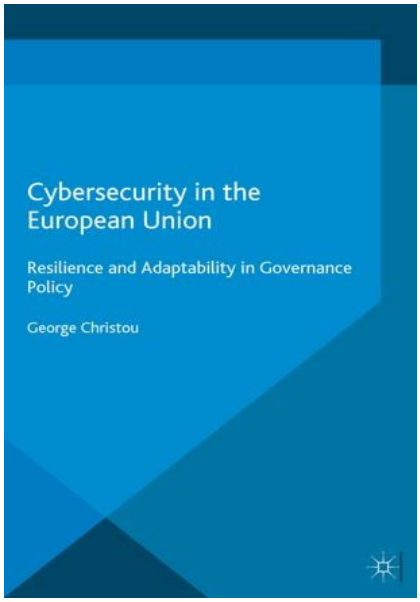
"This book offers a comparative perspective on data protection and cybersecurity in Europe. In light of the digital revolution and the implementation of social media applications and big data innovations, it analyses threat perceptions regarding privacy and cyber security, and examines socio-political differences in the fundamental conceptions and narratives of privacy, and in data protection regimes, across various European countries. The first part of the book raises fundamental legal and ethical questions concerning data protection; the second analyses discourses on cybersecurity and data protection in various European countries; and the third part discusses EU regulations and norms intended to create harmonized data protection regimes. "



EU internet law: regulation and enforcement

Tatiana-Helenē Synodinou ; Philippe Jougleux ; Christiana Markou ; Thalia Prastitou (Eds.)
Cham : Springer International Publishing : Imprint: Springer, 2017
Available at Legal Library Main Collection (SJUR INFORM 104916)

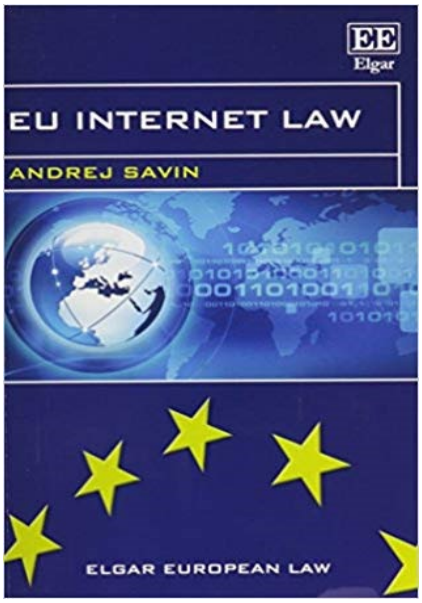
"This book provides an overview of legal developments concerning the digital era, to examine the extent to which law has or will further evolve in order to adapt to its new digitalized context. More specifically it focuses on some of the most important legal issues found in areas directly connected with the Internet, such as intellectual property, data protection, consumer law, criminal law and cybercrime, media law and, lastly, the enforcement and application of law. By adopting this horizontal approach, it highlights – on the basis of analysis and commentary of recent and future EU legislation as well as of the latest CJEU and ECtHR case law – the numerous challenges faced by law in this new digital era."



Cybersecurity in the European Union: resilience and adaptability in governance policy

George Christou
London : Palgrave Macmillan UK : Imprint: Palgrave Macmillan, 2016
Request via Eureka

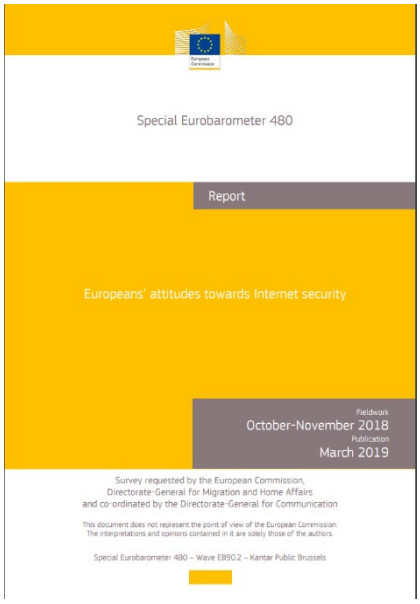
"This book interrogates the European Union's evolving cybersecurity policies and strategy and argues that while progress is being made, much remains to be done to ensure a secure and resilient cyberspace in the future."



EU internet law

Andrej Savin
Cheltenham : Edward Elgar, 2017
Available at Legal Library Main Collection (SJUR INF 104837)

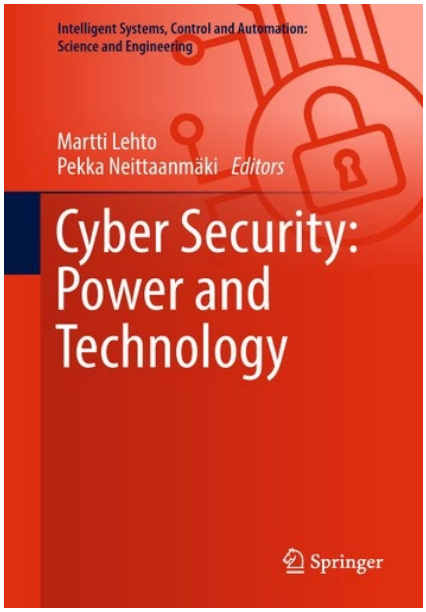
"The modern world has been subject to information and communication technology penetration at an unprecedented level. While the early battles over Internet regulation have largely subsided, the debate around who regulates and when, remains strong. This book gives an overview of EU Internet regulations, as well as evaluates EU policy-making and governance. It begins with a detailed examination of the constitutional context within which the Internet is regulated and the various policy documents that have informed this regulation over the years. It then examines key issues in Internet regulation, including electronic commerce, jurisdiction, content regulation, intellectual property, consumer protection, and criminal regulation."



Europeans' attitudes towards Internet security

European Commission ; Directorate-General for Home Affairs ; Kantar Public Brussels
Brussels : European Commission, 2019
Access via Eureka

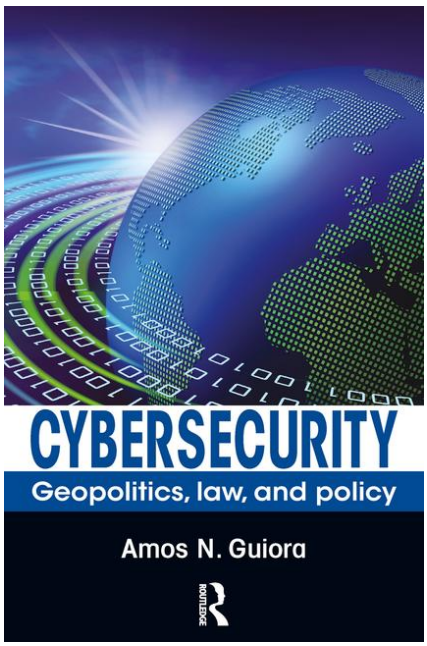
"The aim of the Special Eurobarometer survey is to understand EU citizens' awareness, experiences and perceptions of cyber security issues. This report presents the findings of this survey. It identifies patterns and trends in the frequency of Internet use, the means by which respondents access the Internet, and the kinds of activities that the Internet is commonly used for. It examines concerns of respondents about the security of Internet transactions, the impact these concerns are having on respondents' behaviour, and specifically the impact these concerns are having on the steps respondents take to secure online accounts. The survey concludes with a section that examines respondents' awareness of the existence of official resources for reporting cybercrime, and the actions respondents would take if they were to fall victim to cybercrime."



Cyber security : power and technology

Martti Lehto ; Pekka Neittaanmäki (Eds.)
Cham : Springer, 2018
Available at Council Library Main Collection (105252)

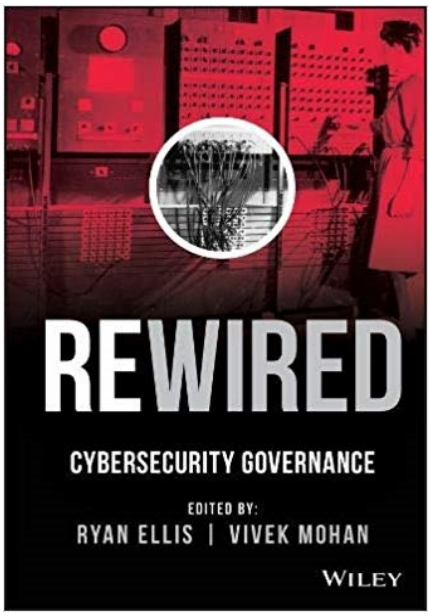
"Addressing open problems in the cyber world, the book consists of two parts. Part I focuses on cyber operations as a new tool in global security policy, while Part II focuses on new cyber security technologies when building cyber power capabilities. The topics discussed include strategic perspectives on cyber security and cyber warfare, cyber security implementation, strategic communication, trusted computing, password cracking, systems security and network security among others."



Cybersecurity: geopolitics, law and policy

Amos N. Guiora
London, England ; New York, New York : Routledge, 2017
Request via Eureka

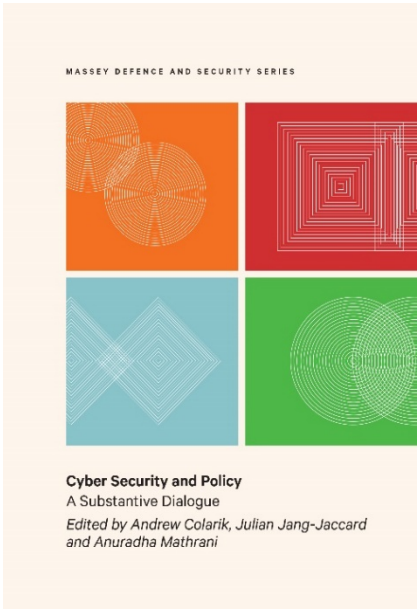
"This book examines the legal and policy aspects of cyber-security. It takes a much needed look at cyber-security from a geopolitical perspective. Through this lens, it seeks to broaden the reader's understanding of the legal and political considerations of individuals, corporations, law enforcement and regulatory bodies and management of the complex relationships between them. The work seeks to highlight the constant threat of cyber-security against various audiences, with the overall aim of facilitating discussion and reaction to actual probable events."



Rewired cybersecurity governance

Ryan Ellis ; Vivek Mohan (Eds.)
Hoboken, NJ : Wiley, 2019
Request via Eureka

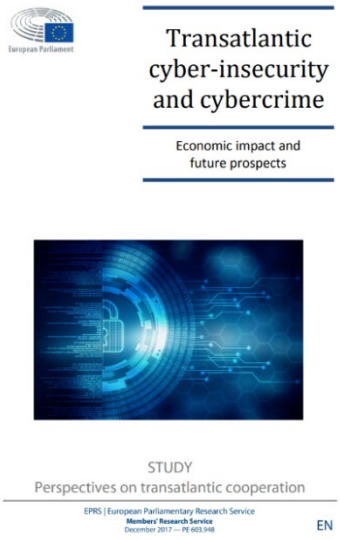
"Through twelve detailed case studies, this collection provides an overview of the ways in which government officials and corporate leaders across the globe are responding to the challenges of cybersecurity. Drawing perspectives from industry, government, and academia, the book incisively analyses the actual issues and provides a guide to the continually evolving cybersecurity ecosystem. It charts the role that corporations, policymakers, and technologists are playing in defining the contours of our digital world. Rewired: Cybersecurity Governance places great emphasis on the interconnection of law, policy, and technology in cyberspace. It examines some of the competing organizational efforts and institutions that are attempting to secure cyberspace and considers the broader implications of the in-place and unfolding efforts–tracing how different notions of cybersecurity are deployed and built into stable routines and practices."



Cyber security and policy : a substantive dialogue

Andrew Colarik ; Julian Jang-Jaccard ; Anuradha Mathrani (Eds.)
Auckland, New Zealand : Massey University Press, 2017
Request via Eureka

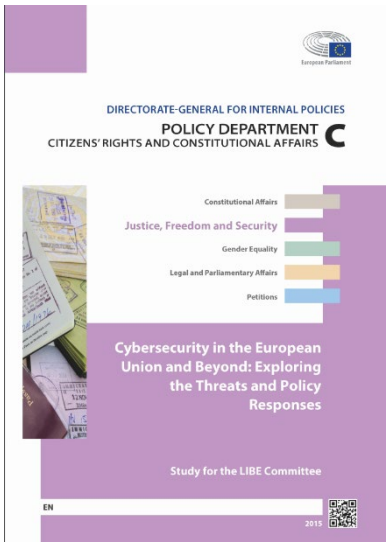
"A world without the advantages and convenience provided by cyberspace and the internet of things is now unimaginable. But do we truly grasp the threats to this massive, interconnected system? And do we really understand how to secure it? After all, cyber security is no longer just a technology problem; the effort to secure systems and society are now one and the same. This book discusses cyber security and cyber policy in an effort to improve the use and acceptance of security services. It argues that a substantive dialogue around cyberspace, cyber security and cyber policy is critical to a better understanding of the serious security issues we face."



Transatlantic cyber-insecurity and cybercrime economic impact and future prospects

Benjamin C. Dean ; European Parliament ; Directorate-General for Parliamentary Research Services
Brussels : European Parliament, 2017
Access via Eureka

"Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has also enabled costly new forms of crime, and created systemic risks to transatlantic and national critical infrastructure, threatening economic growth and development. The transnational nature of these phenomena make it very difficult for effective policy solutions to be implemented unilaterally by any one jurisdiction. Cooperation between stakeholders in both the EU and US is required in the development and implementation of policies to increase the security of digital technologies and increase societal resilience to the cybersecurity risks associated with critical infrastructure. Although there is a great deal of congruence between the stated policy goals in both the EU and US, obstacles to effective cooperation impede effective transatlantic policy development and implementation in some areas. This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues that policy-makers on either side of the Atlantic could work together on, and explains where effective cooperation is sometimes impeded."



Cybersecurity in the European Union and beyond exploring the threats and policy responses

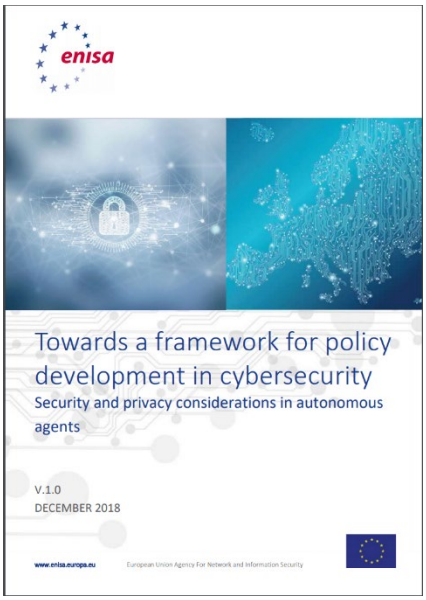
Nicole van Der Meulen ; Eun A Jo; Stefan Soesanto; European Parliament ; Directorate-General for Internal Policies of the Union
Luxembourg : Publications Office, 2015
Access via Eureka

"This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. It sets out to develop a better understanding of the main cybersecurity threats and existing cybersecurity capabilities in the European Union and the United States. The study further examines transnational cooperation and explores perceptions of the effectiveness of the EU response, pinpointing remaining challenges and suggesting avenues for improvement."

State of the Union 2018: building strong cybersecurity in Europe

European Commission ; Directorate-General for Communication
Luxembourg : Publications Office , 2018
Access via Eureka

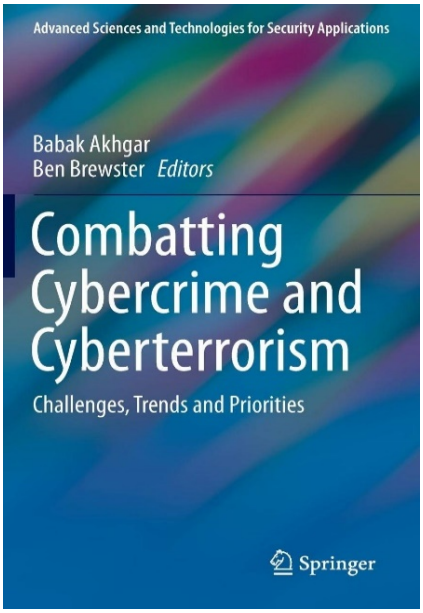
"To equip Europe with the right tools to deal with an ever-changing cyber threat, in 2017 the European Commission and the High Representative proposed a wide-ranging set of measures to build strong cybersecurity in the EU. These efforts are now being complemented by a proposal helping the EU to pool resources and expertise in research and innovation, and to become a leader in the next generation of cybersecurity and digital technologies."



Towards a framework for policy development in cybersecurity security and privacy considerations in autonomous agents

Prokopios Drogkaris ; Athena Bourka ; European Union Agency for Network and Information Security et al.
Heraklion : ENISA, 2018
Access via Eureka

"The objective of the study is on the one hand to provide an overview of representative application domains and on the other hand to contribute and complement relevant initiatives at EU level while also providing relevant insights, both for security and privacy, for future EU policy shaping initiatives."



Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities

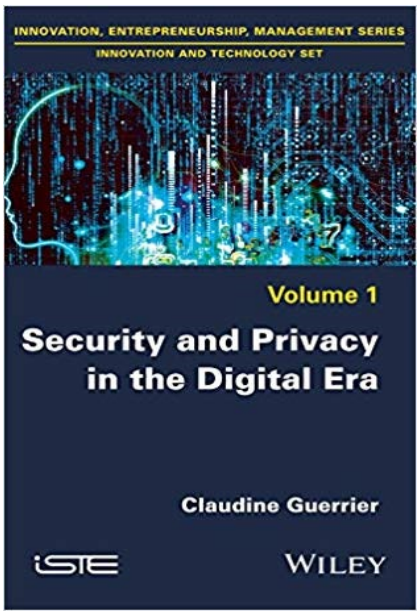
Babak Akhgar ; Ben Brewster (Eds.)
Cham : Springer International Publishing : Imprint: Springer, 2016
Request via Eureka

"This book comprises an authoritative and accessible edited collection of chapters of substantial practical and operational value. For the very first time, it provides security practitioners with resource designed to guide them through the complexities and operational challenges associated with the management of contemporary and emerging cybercrime and cyberterrorism (CC/CT) issues. Benefiting from the input of three major European Commission funded projects the book's content is enriched with case studies, explanations of strategic responses and contextual information providing the theoretical underpinning required for the clear interpretation and application of cyber law, policy and practice, this unique volume helps to consolidate the increasing role and responsibility of society as a whole, including law enforcement agencies (LEAs), the private sector and academia, to tackle CC/CT."

Cybercriminalité : état des lieux

Frédéric Dechamps ; Caroline Lambilot
Limal : Anthemis, 2016
Available at Legal Library Main Collection (SJUR INF 103353)

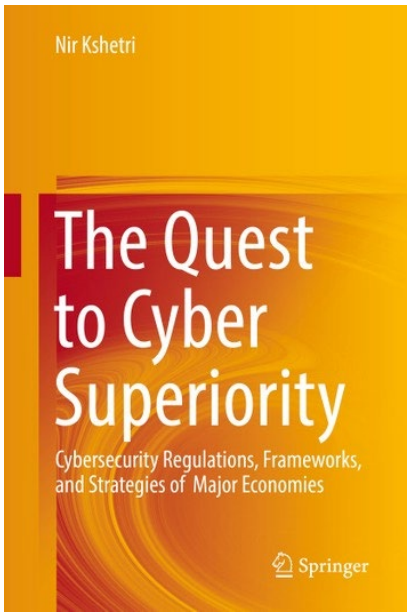
"Qu'est-ce que la cybercriminalité? Comment est né et a évolué ce phénomène? Comment le droit l'appréhende-t-il? Quelles sont les méthodes mises en place afin d'y répondre efficacement? Quels sont les risques liés à l'utilisation des moyens informatiques pour les entreprises? Ces questions, et tant d'autres, ont amené les auteurs, tous deux avocats au barreau de Bruxelles, à rédiger cet ouvrage. C'est à la lumière, d'une part, d'un développement théorique et, d'autre part, d'une mise en perspective pratique et concrète qu'ils tentent d'apporter quelques réponses. Par ce livre, nous invitons le lecteur à devenir (ou rester) un internaute critique et éclairé."



Security and privacy in the digital era. Volume 1

Claudine Guerrier
London, England ; Hoboken, New Jersey : ISTE : Wiley, 2016
Request via Eureka

"This book will examine the security/freedom duo in space and time with regards to electronic communications and technologies used in social control. It will follow a diachronic path from the relative balance between philosophy and human rights, very dear to Western civilization (at the end of the 20th Century), to the current situation, where there seems to be less freedom in terms of security to the point that some scholars have wondered whether privacy should be redefined in this era."



The quest to cyber superiority cybersecurity regulations, frameworks, and strategies of major economies

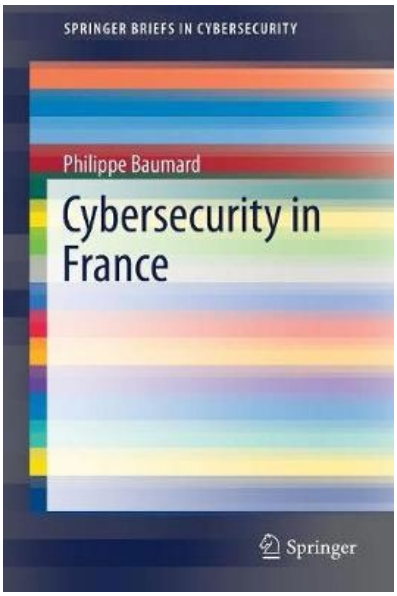
Nir Kshetri
Cham : Springer International Publishing : Imprint: Springer, 2016
Request via Eureka

"This book explains how major world economies are recognizing the need for a major push in cyber policy environments. It helps readers understand why these nations are committing substantial resources to cybersecurity, and to the development of standards, rules and guidelines in order to address cyber-threats and catch up with global trends and technological developments."

Cyber-Sicherheit

Hans-Jürgen Lange ; Astrid Bötticher
Wiesbaden : Springer Fachmedien Wiesbaden, 2014
Access via Eureka

"Die technikvermittelte Kommunikation wird immer wichtiger. Diese Entwicklung wurde zum Anlass genommen, die diversen Aspekte der Cyber-Sicherheit aus disziplinübergreifender Perspektive zu untersuchen. Der strukturelle Wandel, der sich aus den Implikationen der Informationsgesellschaft ergibt, die Handlungsgrenzen der Institutionen, Organisationen und verschiedenen Akteure der Gesellschaft sowie Fragen der Cybersicherheit sind die Themen, die diese Publikation in einem interdisziplinären Zusammenspiel aufgreift."



Cybersecurity in France

Philippe Baumard
Cham : Springer International Publishing : Imprint: Springer, 2017
Access via Eureka

This book presents the overarching framework in which each nation is developing its own cyber-security policy, and the unique position adopted by France. By analysing the particular case of France national strategy and capabilities, the authors investigate the difficulty of obtaining a global agreement on the regulation of cyber-warfare. A review of the motives for disagreement between parties suggests that the current regulation framework is not adapted to the current technological change in the cybersecurity domain. This book suggests a paradigm shift in handling and anchoring cyber-regulation into a new realm of behavioural and cognitive sciences, and their application to machine learning and cyber-defence."

Selected articles

Responding to cyberattacks prospects for the EU cyber diplomacy toolbox
Paul Ivan
European Policy Centre, 2019

"The paper analyses the development of the EU's diplomatic response to malicious cyber activities, the challenges that hamper a common EU response and possible ways to address these challenges. It focuses on issues linked to the attribution of cyberattacks and on the most powerful diplomatic instrument to be adopted to respond to them: the use of cyber sanctions."

Challenges to effective EU cybersecurity policy
European Court of Auditors, March 2019

"The objective of this briefing paper, which is not an audit report, is to provide an overview of the EU's complex cybersecurity policy landscape and identify the main challenges to effective policy delivery. It covers network and information security, cybercrime, cyber defence and disinformation. The paper will also inform any future audit work in this area."

Strengthening the EU's cyber defence capabilities
Melissa K. Griffith
Centre for European Policy Studies, 2018

"The EU's current cyber defence capacity remains fragmented across various institutions and agencies. After a comparative analysis of alternative scenarios, this paper concluded in favour of creating an EU Cyber Defence Agency with executive competencies and therefore, the ability to develop and utilise strategic and operational capabilities at the EU level. This would mark a critical step towards a more effective and collaborative approach to enhancing cyber security and resilience in the EU."

Cybersécurité des infrastructures énergétiques regards croisés Europe/États-Unis
Arnault Barichella
Institut français des relations internationals, 2018

Abstract in English: "The acceleration of the digitization of energy infrastructures brings many economic benefits, especially in terms of rationalization of energy consumption with efficiency gains. However, this also increases the risk of cyber-attacks, where malware is taking advantage of the increasing digitization of equipment. Recent cyber-attacks targeting Ukrainian critical infrastructure point to the threat as real and growing. Vulnerability is not confined to infrastructure located in the European Union or the United States: some of the attacks on Ukraine have spread

to many Western companies including through their subsidiaries, highlighting the danger of contagion through malware."

Kyberterrorismin uhka Euroopassa

Tommi Laari
University of Jyväskylä informaatioteknologian tiedekunta, 2018

Abstract in English: "Cyberterrorism has been named one of the world's most serious security threats in the future. The aim of this study was to explain the cyberterrorism, the threat it poses, and how this threat is perceived from the point of view of European states. The main research question has been: What kind of threat is cyber terrorism in Europe? Though terrorism is strongly exposed in daily news coverage, terrorist and cyber terrorism in the European states' cybersecurity strategies is handled very narrowly. However, terrorist attacks in recent years have led the authorities to worry more about this emerging terrorist sector, cyberterrorism".

Cybersecurity in the EU Common Security and Defence Policy (CSDP): challenges and risks for the EU

Panagiotis Trimintzios, Georgios Chatzichristos, Silvia Portesi et al.
European Parliament Think Tank, 2017

"This study is the result of a study conducted by the European Union Agency for Network and Information Security (ENISA) for the European Parliament's Science and Technology Options Assessment (STOA) Panel with the aim of identifying risks, challenges and opportunities for cyber-defence in the context of the EU Common Security and Defence Policy (CSDP). The study revolves around three thematic areas, namely: policies, capacity building, and the integration of cyber in the CSDP missions, with the last one being the main focus of the study. For each thematic area, we compile a set of policy options, covering different levels, starting from the EU's political/strategic level and progressing down to the operational and even tactical/technical levels of the CSDP's supporting mechanisms."

Das neue »Europa der Sicherheit«

Annegret Bendiek
Stiftung Wissenschaft und Politik, 2017

"Im Juli 2017 übernimmt Estland den Vorsitz im Rat der EU. Est-lands Hauptthemen werden die Digitalisierung sowie Europas gemeinsame Außen-, Sicherheits- und Vertei-digungspolitik sein. Damit greift die Ratspräsidentschaft wichtige Herausforderungen für Europa auf. Gleichzeitig kann sie ein weit geöffnetes Gelegenheitsfenster nutzen, denn die Regierungen der EU-Mitgliedstaaten betrachten eine Vertie-fung europäischer Außen- und Sicherheitspolitik heute wohlwollender als

jemals zuvor. Auch der Kom-mission ist das Thema Sicherheit seit Beginn ihrer Amtszeit ein ständiges Anliegen – von Kommissions-präsident Junckers' Politischen Leitlinien vom Juli 2014 bis zu seiner vorerst letzten Rede zur Lage der Union im Septem-ber 2016. Politik und Gesell-schaft unterstützen ein »Europa der Sicherheit«, das auf drei Großprojekten aktueller Europa-politik aufbaut: einer Sicherheitsunion, einer Verteidigungsunion und einer engen Zusammenarbeit zwischen Nato und EU. Beim Schutz kritischer Infra-strukturen, also in der Cybersicherheit, verschmelzen diese Projekte. Alle drei sollten in einem übergrei-fen-den Weißbuch mit einer gemeinsamen strategischen Ausrichtung versehen werden."

Strengthening the EU's cyber defence capabilities

Jaap de Hoop Scheffer ; Lorenzo Pupillo ; Melissa K. Griffith ; Steven Blockmans ; Andrea Renda
Centre for European Policy Studies, 2018

"Cyber defence is critical to both the EU's prosperity and security. Yet, the threat space it faces is vast in scope, highly interconnected, deeply complex, and rapidly evolving. The EU's current cyber defence capacity remains fragmented across and siloed within various institutions, agencies. In order to secure its own use of cyberspace, the EU must be bold. The CEPS Task Force on Strengthening the EU's Cyber Defence Capabilities identified a clear EU-wide interest for greater coordination and cooperation in this space. After a comparative analysis of alternative scenarios, the Task Force concluded in favour of creating an EU Cyber Defence Agency with executive competencies and therefore, the ability to develop and utilise strategic and operational capabilities at the EU level. This would mark a critical step towards a more effective and collaborative approach to enhancing cyber security and resilience in the EU."

EU cyber partnerships assessing the EU strategic partnerships with third countries in the cyber domain

Thomas Renard
Egmont – Royal Institute for International Relations, 2018

"The European Union is increasingly active on cyber issues internationally, guided by its various foreign policy documents and strategies, including its 2013 Cybersecurity Strategy and the 2015 Council conclusions on cyber-diplomacy. In line with these documents, the EU has deepened its bilateral ties with a number of key countries, resulting in a network of cyber partnerships. This article explores these partnerships in depth. It seeks to explain the different types of purposes that they fulfil, and the various mechanisms that underpin them, based on an ambitious mapping exercise."

Cybersecurity culture guidelines: behavioural aspects of cybersecurity

Hague Security Delta ; European Union Agency for Network and Information Security ; European Network and Information Security Agency, 2018

"This study has conducted four evidence-based reviews of human aspects of cybersecurity. Based on the findings of the reviews, this paper proposes a model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity. The report concludes with recommendations for specific groups such as policy makers, management and organizational leaders, security specialists, software developers and awareness raising managers."

Public–private partnerships on cyber security: a practice of loyalty

Kristoffer Kjærgaard Christensen ; Karen Lund Petersen
International Affairs, 2017, Vol. 93(6), pp.1435-1452

"The governance of cyber-security risks is seen as increasingly important to the security of the nation. However, cyber-security risks are characterized by a fundamental uncertainty, which poses a great challenge to their governance and calls for new modes of organizing security politics. Public–private partnerships (PPPs) are often seen as the answer to this challenge by enhancing flexibility and robustness through knowledge-sharing. Engaging with the literature on PPPs and the Danish practice on cyber security, we show how PPPs involve controversies over different threat realities of cyber security. This plays out as controversies over what is considered threatened, the scope of the issue and the kind of expertise to be mobilized. Arguing that PPPs on security are not defined narrowly by short-sighted strategic self-interest but also loyalty and commitment, we suggest that the innovative potential of such PPPs lie not in a possible consensus on a common purpose and threat reality, but in the ability to embrace divergent definitions and approaches to cyber security. Acknowledging the corporate interests and loyalty, we suggest a move towards the notion of partnering through dissent."

Cyberattaques et systèmes énergétiques: faire face au risque

Gabrielle Desarnaud
Institut français des relations internationales, 2017

Abstract in English: "This study analyses the risks of cyber-attacks on European energy infrastructures, as well as their potential consequences, notably on power grids. It offers a comparative approach to the measures taken by different European countries to protect their industry and to collaborate at EU level."

Good neighbours make good security: coordinating EU critical infrastructure protection against cyber threats

Philip Chertoff
GLOBSEC Policy Institute, 2017

"This paper examines the current vulnerability of EU critical infrastructure to failures caused by cyberattacks. It introduces the theory and implications of critical infrastructure interdependencies and explores past EU efforts to secure critical infrastructure from physical failures. Accounting for the damage and versatility cyberattacks on critical infrastructure, this paper suggests that the recently adopted "Directive on security of network and information systems" (NIS Directive), which aims to mitigate cyber-threats to critical infrastructure, will not be sufficient to handle the possible cross-industry and cross-border impacts of cyberattacks on critical infrastructure."

Strengthening the EU's resilience in the virtual domain

Gonçalo Carriço
Wilfried Martens Centre for European Studies, 2017

"This paper analyses the unstoppable phenomenon of globalisation through the lens of cyberspace. It looks at how the threats associated with this domain could evolve into a cyberwar. The paper assesses the EU's stance on cyberspace and elaborates the directions that the EU should develop and pursue in this regard."

The EU as a coherent (cyber)security actor?

Helena Carrapico ; André Barrinha
JCMS: Journal of Common Market Studies, November 2017, Vol.55(6), pp.1254-1272

"The last three decades have seen the development of the European Union (EU) as a security actor. The transnational character of the security threats and the challenges identified by the EU have led to progressive integration between internal and external security concerns. These concerns have often led to calls for greater coherence within EU security policies. The literature, however, indicates that this need for coherence has, so far, not been systematically operationalized, leading to a fragmented security field. This article has two main aims: To devise a framework for the analysis of the EU's coherence as a security actor, and to apply it to the cybersecurity field. By focusing on EU cybersecurity policy, this article will explore whether the EU can be considered a coherent actor in this field or whether this policy is being implemented according to different and unco-ordinated rationales."

Relanzamiento del plan de ciberseguridad de la UE

Javier Alonso Lecuit
Real Instituto Elcano, 2017

Abstract in English: "The present article analyses the Commission proposal of a comprehensive set of measures to address the escalation of cybercrime and cyber threats."

Strengthening the EU's resilience in the virtual domain

Gonçalo Carriço
Wilfried Martens Centre for European Studies, 2017

"This paper analyses the unstoppable phenomenon of globalisation through the lens of cyberspace. It looks at how the threats associated with this domain could evolve into a cyberwar. The paper assesses the EU's stance on cyberspace and elaborates the directions that the EU should develop and pursue in this regard."

Building an effective European cyber shield: taking EU cooperation to the next level

European Political Strategy Centre, 2017

"Breaches of sensitive data, mass disinformation campaigns, cyberespionage and attacks on critical infrastructure – these are no longer futuristic threats, but real events that affect individuals, businesses and governments on a daily basis. Yet they remain largely unprosecuted. Though so far below the threshold of outright war, cyber aggression is emerging as a major new vector that can be activated to achieve strategic superiority, destabilise states, and cause large-scale economic damage."

Die erneuerte Strategie der EU zur Cybersicherheit

Annegret Bendiek ; Raphael Bossong ; Matthias Schulze
Stiftung Wissenschaft und Politik, 2017

"Im September 2017 hat die EU ihre Strategie zur Cybersicherheit aus dem Jahr 2013 aktualisiert. Damit soll Europas kritische Infrastruktur besser geschützt und die digitale Selbstbehauptung gegenüber anderen Weltregionen befördert werden. Doch die erneuerte Strategie lässt Fragen offen, wenn es darum geht, die selbstgesetzten Ziele eines »offenen, freien und sicheren Cyberraums« nach innen wie außen glaubhaft zu vertreten. Weder formuliert die EU eine klare Definition von Widerstandskraft und Abschreckung, noch wird deutlich genug, wie die institutionelle Fragmentierung und rechtliche Unverbindlichkeit in Cybersicherheitsfragen auf EU-Ebene überwunden werden sollen. Zudem bleiben kontroverse Themen ausgespart, wie die Harmonisierung des Strafrechts oder die Nutzung von Verschlüsselung. Die Mitgliedstaaten sollten

ihre nationalen Alleingänge aufgeben und die gesetzliche Regulierung zur Cybersicherheit auf Ebene der Union beschleunigen."

Warring from the virtual to the real: assessing the public′s threshold for war over cyber security

Sarah Kreps ; Debak Das
Research & Politics, June 2017, Vol.4(2)

"Accusations of Russian hacking in the 2016 US presidential election has raised the salience of cyber security among the American public. However, there are still a number of unanswered questions about the circumstances under which particular policy responses are warranted in response to a cyber-attack and the public's attitudes about the conditions that justify this range of responses. This research investigates the attributes of a cyber-attack that affect public support for retaliation. It finds that cyber-attacks that produce American casualties dramatically increase support for retaliatory airstrikes compared to attacks with economic consequences. Assessments of attribution that have bipartisan support increase support to a lesser extent but for a broader range of retaliatory measures. The findings have important implications for ongoing debates about cyber security policy."

L'espace numérique et la protection des données personnelles au regard des droits fondamentaux

Henri Oberdorff
Revue du droit public et de la science politique en France et à l'étranger. No. 1 (2016), pp. 41-54

"Ces dernières années, les études et les rapports se sont multipliés, soit pour vanter tous les mérites de l'avènement et de la généralisation du numérique, soit pour dénoncer les risques de remise en cause des libertés par cette nouvelle technologie. Ces deux types de point de vue s'expliquent compte tenu des ambivalences de l'espace numérique face aux libertés. En effet, incontestablement la société numérique débouche sur un accroissement des libertés individuelles ou collectives. Des espaces numériques de liberté complètent ceux qui existent déjà. En même temps, les libertés individuelles ou collectives se trouvent simultanément menacées justement par ces technologies. Leurs utilisations abusives peuvent se révéler contraires aux droits de l'homme et aux libertés fondamentales."

EUnited against crime: improving criminal justice in European Union cyberspace

Tommaso De Zan ; Simona Autolitano
Istituto Affari Internazionali, 2016

"In today's ultra-connected world, much of our life occurs online. Despite the benefits generated by increased connectivity and more powerful processing tools, ICT systems have not only been

employed to foster social and economic development. Terrorists and cybercriminals are increasingly using cyberspace to conduct their malfeasances. In June 2016, the Council of the EU underlined the importance of improving the effectiveness of criminal justice in cyberspace. Using the Council conclusions as a starting point, the paper provides some "policy suggestions" for the ongoing debate taking place within EU institutions."

Cyber-Security aus Sicht der Sicherheitspolitik

Johannes Klick ; Stephan Lau ; Daniel Marzin
Freie Universität Berlin ; Open Competence Center for Cyber Security, 2015

"Dieser Studienbrief gibt Ihnen einen Einblick in die Sicherheitspolitik. Sie werden erfahren wie Sicherheit aus politischer und informationstechnischer Sicht definiert ist. Anschließend lernen Sie die Gründe für den Wandel der Sicherheitspolitik der vergangenen Jahrzehnte kennen. Dies hilft Ihnen zu verstehen, vor welchen Herausforderungen die Sicherheitspolitik im Bereich Cyber-Security steht."

Cybersecurity in the European Union and beyond: exploring the threats and policy responses

Nicole van der Meulen ; Eun A Jo ; Stefan Soesanto et al.
RAND Europe. ; European Parliament. Directorate-General for Internal Policies of the Union, 2015

"This study sets out to develop a better understanding of the main cybersecurity threats and existing cybersecurity capabilities in the EU and the US. The study further examines transnational cooperation and explores perceptions of the effectiveness of the EU response, pinpointing remaining challenges and suggesting avenues for improvement."

Improving cyber security: NATO and the EU

Piret Pernik
Rahvusvaheline Kaitseuuringute Keskus, 2014

"The critical infrastructure and essential services on which modern economies depend, rely increasingly on information and communication technologies. Most global, transatlantic and regional international organisations have developed policies and instruments to address the growing sophistication of cyber-attacks against critical infrastructures and services. This paper presents a comparative analysis of the approaches of NATO and the EU to cyber security."