Policy Design and Practice

Routledge
Taylor & Francis Group

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rpdp20

Governing cyber crises: policy lessons from a comparative analysis

François Delerue & Monica Kaminska

To cite this article: François Delerue & Monica Kaminska (2023) Governing cyber crises: policy lessons from a comparative analysis, Policy Design and Practice, 6:2, 127-130, DOI: 10.1080/25741292.2023.2213061

To link to this article: https://doi.org/10.1080/25741292.2023.2213061

Published online: 16 May 2023.

POLICY DESIGN AND PRACTICE
2023, VOL. 6, NO. 2, 127–130
https://doi.org/10.1080/25741292.2023.2213061

Routledge
Taylor & Francis Group

INTRODUCTION

OPEN ACCESS Check for updates

Governing cyber crises: policy lessons from a comparative analysis

François Delerue[a] and Monica Kaminska[b]

[a]IE Law School, IE University, Madrid, Spain; [b]The Hague Program on International Cyber Security, Institute for Security and Global Affairs, Leiden University, The Hague, The Netherlands

ARTICLE HISTORY Received 2 May 2023; Accepted 3 May 2023

In cyberspace, the notion of crisis is multifaceted. The complexity of cyber crises pertains to the diversity of actors, activities, targets, and effects involved, creating governance challenges. For example, information campaigns on the Internet have created a crisis of trust in political discourse and authority in many democratic societies. A recent ransomware attack by a criminal actor brought the entire nation of Costa Rica to a standstill. Incidents such as the state-sponsored SolarWinds and Microsoft Exchange hack have put pressure on the demarcation line between cyber espionage and disruptive cyber operations. Strategic shifts to more proactive and continuous operations as a method of addressing cyber conflict short of war raise questions about key concepts like sovereignty and breed concerns about crisis escalation. State-sponsored malware is increasingly being found in critical infrastructure and electoral systems. The current armed conflict in Ukraine, which has seen an unprecedented involvement of cyber hacktivist groups and private actors, brings to the fore new difficulties of cyber crisis management for both the belligerents and third states. These ongoing developments in the threat landscape continually shift the goal posts on acceptable state behavior in cyberspace.

Despite important strides in cyber policy development by some governments, many strategies are still in the early stages of maturity and provide little guidance for the diversity of cyber crises that can unfold. Moreover, there is much variance in national, regional, and multilateral approaches to what is sometimes called a cyber "wild west" in the international realm, yet these divergences remain understudied. Additionally, states do not always abide by their own policies or the ones agreed internationally, both in their practice of offensive cyber operations and in addressing

CONTACT Monica Kaminska m.k.kaminska@fgga.leidenuniv.nl The Hague Program on International Cyber Security, Institute for Security and Global Affairs, Leiden University, The Hague, The Netherlands
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

crises. Discrepancies between cyber policy and practice merit greater political and scholarly attention. Building on these observations, this Special Issue investigates different policy approaches to managing cyber crises and proposes alternative policy frameworks to guide policy-makers and practitioners in addressing novel threats.

This Special Issue is comprised of six articles and gathers a diverse group of thinkers in the field to examine a series of topics relating to how "crisis" translates into cyberspace, notably from the point of view of policy development, capability management, and the applicable legal frameworks.

The first article, by Tobias Liebetrau, focuses on capability management, developing three models for the organization of cyber capabilities between intelligence services and military entities, based on three European country case studies. Liebetrau argues that the choice of organizational model can have powerful shaping effects on the intelligence agencies and military entities themselves with overall positive implications for achieving broader strategic goals. Nevertheless, he calls for more political and public debate about the organization of national cyber capabilities and more transparency about their operational conduct in addressing cyber conflict short of war.

The second article by Nnenna Ifeanyi-Ajufo provides a much-needed analysis of African cyber governance and examines whether states in the region will be able to meet the objectives in the African Digital Transformation Strategy. The article casts doubt on whether existing policies and infrastructure can ensure the region's cyber resilience. For the potential of digital technologies to be realized on the continent, states need to prioritize cybersecurity and related legislation that is sensitive to cultural differences and domestic capabilities; develop better cooperation mechanisms both between states and between sub-regional organizations; and eventually come up with shared conceptual understandings and norms of behavior in cyberspace.

In the third article, Gareth Mott, Jason Nurse, and Christopher Baker-Beall explore the cybersecurity lessons that the United Kingdom can draw from the governance of the Coronavirus (SARS-CoV-2) pandemic. The article focuses particularly on mitigating threats to critical systems, addressing societal harms, and devising appropriate communications strategies. Building on an assessment of recent British cyber security strategies and the government's handling of ransomware attacks, the article highlights as a key argument that more nuanced, dynamic, and empathetic multi-stakeholder engagement is necessary to be prepared for future cyber crises.

The fourth article by Mischa Hansel takes a broader view: it analyses the narrative developed by certain Great Powers to explain the international community's recurrent failures in cyber norms building processes. Focusing in particular on the policy agendas and narratives of the United States and the Russian Federation, Hansel studies how states engage in intense public diplomacy competition and legitimization strategies, seeking to escape and divert blame from their norms building failures. The article's discussion and analysis of policy implications go beyond the cases of the United States and the Russian Federation, urging readers to pay more attention to the narrative dimensions of public diplomacy and the delegitimization risks that

particular portrayals of cyber governance processes can breed. Hansel notably advocates for clearer referencing to the norms developed at the UN level in state practice, in particular in state public attribution statements, in order to enhance the legitimacy of international cyber security policy-making.

The fifth article by June Lee focuses on the strategic rationale for public attribution and provides some early indications for why we might not be witnessing the clear referencing to UN cyber norms, despite the merits of this approach identified by Hansel. Lee investigates the United States' policy of publicly attributing cyber incidents, providing an interpretive taxonomy for how and under what circumstances the United States engages in attribution. Lee cautions that differing organizational interests mean that there is often a lack of a unified approach to attribution across the U.S. government, which can raise challenges for U.S. cyber diplomacy and shape the development of international norms in unanticipated ways.

The sixth article by Ferry Oorsprong, Paul Ducheine, and Peter Pijpers tackles one of the most pressing legal and policy challenges facing states: when does a cyber operation cross the threshold of "armed attack" under international law? It is by now an uncontroversial statement that the most severe forms of cyber operations may be considered an armed attack, allowing for the invocation of the right to self-defense. Yet, there is no agreed definition of the threshold of "armed attack" and no clear guidance for such in the academic literature. This article aims to close this gap by proposing an original policy framework for The Netherlands, which can serve as a guideline for determining when a cyber operation qualifies as an armed attack and would thus allow for the invocation of the right to self-defense.

The variety of articles in this Special Issue reflects the diversity of cyber crises and the governance dilemmas they raise. A series of general observations can be drawn from them, to which we now turn. Firstly, the diversity of forms of cyber crisis calls for a holistic approach to the development and implementation of state policies. Its benefits are highlighted by Mott et. al.'s comparative analysis of cyber crises and the Coronavirus pandemic. We can and should learn lessons from other policy areas outside of cyber security.

Secondly, in state policy and practice, there exist inconsistencies and tensions in the relationship between legal obligations relating to the application of international law to cyberspace and non-binding policy norms, notably developed within UN-led international discussions. This Special Issue offers some insights on the necessity of reconciling these different sources of state policies and practices, both at the national and international level. Moreover, states should pay attention to the potential legal implications of their activities and ensure that they don't undermine the international rules based order with inconsistent policies.

Thirdly, the articles in this Special Issue illuminate divergent national and regional approaches to the management of cyber crises and threats. Given the still relative immaturity of the cyber studies field and its strong focus on general theories for understanding and managing cyber conflict, we hope that these articles will provide an important ice-breaker for more scholarship on national and regional policies on these issues.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

François Delerue http://orcid.org/0000-0002-6117-6187
Monica Kaminska http://orcid.org/0000-0001-6729-5235