2023-01

Land, sea, air and the cloud: the fourth border type

Starkey, Victoria

Master in International Relations, Strategy and Security, School of Social Sciences, Arts and Humanities, Neapolis University of Pafos

JANUARY 2023

SCHOOL OF SOCIAL SCIENCES, ARTS AND HUMANITIES

DEPARTMENT OF HISTORY, POLITICS AND INTERNATIONAL STUDIES

LAND, SEA, AIR AND THE CLOUD: THE FOURTH BORDER TYPE

VICTORIA STARKEY

JANUARY/2023

SCHOOL OF SOCIAL SCIENCES, ARTS AND HUMANITIES

DEPARTMENT OF HISTORY, POLITICS AND INTERNATIONAL STUDIES

LAND, SEA, AIR AND THE CLOUD: THE FOURTH BORDER TYPE

This thesis was submitted for distance acquisition of a postgraduate degree International Relations, Strategy and Security at Neapolis University

VICTORIA STARKEY

JANUARY/2023

RESPONSIBLE STATEMENT

I, Victoria Starkey, knowing the consequences of plagiarism, declare responsibly that this paper entitled “Land, Sea, Air and the Cloud: The Fourth Border Type”, the points where I have used ideas, text and/or sources of other authors are clearly mentioned in the text with the appropriate reference and the relevant reference is included in the section of the bibliographic references with a full description.

Victoria Starkey
January 23rd, 2022
Vienna, Austria

Contents

Student Name: Victoria Starkey

Postgraduate Thesis Title: Land, Sea, Air and the Cloud: The Fourth Border Type

This Master's Thesis was prepared during the studies for the distance master's degree at Neapolis University and was approved on 27 January 2023 by the members of the Examination Committee.

Examination Committee:

First Supervisor (Neapolis University Pafos): Efstathios T. Fakiolas, Assistant Professor

Member of the Examination Committee: Marios Evriviades, Deputy Head of the Department of History, Politics and International Studies

Member of the Examination Committee: Dr. Mersilia Anastasiadou, Assistant Coordinator

Glossary

AI ..... Artificial Intelligence
BCP ..... Border Crossing Point
BM ..... Border Management
CERT ..... Computer Emergency Response Teams
CTA ..... Clandestine Transnational Actor
EC ..... European Commission
EU ..... European Union
GDPR ..... General Data Protection Regulation
IBM ..... Integrated Border Management
IP ..... Internet Protocol
JCU ..... Joint Cyber Unit
LEA ..... Law Enforcement Agency
VPN ..... Virtual Private Network

Abstract

The border management of states is tasked with preserving the security of the state at its entry and exit points. Until recently, threats were mainly of physical nature, thus the state border was guarded at physical border crossing points over land, by sea, or from the air. However, the growth of cyberspace and criminal opportunity it brings to creating virtual external threats has shaken the security model. This thesis aims to present how and why cybersecurity should be merged with pre-existing border management structures within states in order to create a holistic security approach for its external borders; both physical and virtual. This requires the advent of a fourth border type and its safeguarding measures, which I refer to as the cloud. The intersection of border management and cybersecurity already exists in many areas but has been largely unexamined as of yet, and where differences exist, such as private sector interest and state regulation, cybersecurity can draw from the institutional memory of the ancient border management sector as a strength. With the rising instability across Europe, hybrid threats are becoming inextricably intertwined with state security and therefore must be countered with a hybrid border approach, which is to say, safeguarding of the cloud border using border management strategy.

Keywords: Border management, cybersecurity, national security, digital sovereignty, EU external borders, integrated border management, hybrid threats, instrumentalization

Land, Sea, Air and the Cloud: The Fourth Border Type

Chapter 1 – Introduction

Traditional border management addresses flows, networks and systems of passage and security at national boundaries, which are demarcated by territorial intersections, namely land borders, airports and airspace, and sea. However, an increasing challenge to national sovereignty is the abstract threat presented in the largely-unguarded cyberspace (Jupillat, 2015; De Spiegeleire, Jans & Rujan, 2017; Goel, 2020; Sargana, Sargana & Anns, 2020). Border management (BM) has always been about preventing direct threats from entering a state's borders, whereas potential cybercrime can make the same types of threats to the state without ever physically trespassing (Weimann, 2004; Carrapico & Barrinha, 2017). In this paper, I will examine whether traditional strategies of "land", "sea" and "air" border management can be applied to confront these external threats through cyberspace despite the entirely intangible nature of the arena, against the backdrop of border management's usually concrete landscape. If it can be demonstrated that existing border management structures can be used to confront cyberattacks by external actors, then clearly a fourth border type should be acknowledged: land, sea, air and the cloud.

1.1 Literature Review

Drawing on literature in these fields, much is said on the topic of border management, as well as on cybersecurity, but a significant gap exists when it comes to the intersection of both. Here I note that I refer to the term 'cybersecurity' frequently as a shorthand reference to a state's threshold of protecting against national threats from cyber-attacks or methods of threat via cyberspace. Therefore, the literature is consulted to guide the reader through the existing political and theoretical frameworks surrounding cybersecurity and border management, where they converge and opportunities for collaboration, and proposals for the way forward.

I would also like to address the use of a particular term I've come across often in my research. Border management by definition assumes an international context, as it works with users crossing in or out of the state (ostensibly to/from another country), which is also a key element of monitoring national cyber security, in which external, international threats must be checked and controlled. In that sense, the word "borderless" is almost meaningless hyperbole because it can almost always be better replaced with "cross-border" instead. The term 'borderless' may support generic policy that applies everywhere to an even standard, but it is imprudent to claim a one-size-fits-all solution is possible in our complicated world. It is therefore more fitting to use the term 'cross-border' as it makes room for tailored approaches to hybrid cyber policy.

Traditional border management is much more widely studied and sourced than cyber management. From the outset, almost all border-related literature speaks of evolving threats at borders, so perhaps 'traditional' is a false term, although in newer works it is used to encompass a time when threats were purely of a physical nature. Glimpses of the ever-evolving responsibilities of border management have always been apparent, as border management itself is an ancient topic that dates back to the very birth of statehood. From the issues of English border demarcations as described by Moore (1899) and Lapsley (1900), to the nuclear question such as discussed by Thornton (1963), to *uti possidetis* discussed by Kocs (1995) and Ratner (1996) to the present topic of this paper, evolving challenges at the border is a common thread through the ages. Authors in demarcation topics are able to refer back to key events in history to make predictions or form theories for forward-looking analysis.

On the other hand, cybersecurity is a new topic that only presented with the advent of the internet, and challenges are evolving with rapid-fire. As of yet, I could not identify any common founding theory or author who is the decisive birther of a universally-accepted 'cybersecurity theory', in the way that many political theories have distinct inventors[1]. Boeke & Broeders (2017, p.1-2) made a similar observation and attempts to develop these missing theoretical approaches to securing cyberborders of states. Due to that lack of historical discussion, many scholarly articles in cybersecurity orient themselves by anchoring the analysis of current cyber-events or news stories against technical and computer science studies to provide explanations, while possibly tying in current (failed or recommended) state policy to overcome the attack. Examples are the works of Boeke & Broeders (2018) and Kapucu & Hu (2022) who refer to the technical works of Provan & Kenis (2008) on network systems to develop their arguments, or Jain *et al*. (2006), Zhu (2017), and Vincent (2021), who rely on the research of Uludag *et al*. (2004) on biometric technology to discuss implications.

The overlap – this so-called cloud border – seems to be severely under-examined, although there is indeed an uptick in interest in recent years, especially under the umbrella of hybrid threats (Hoffman, 2014; Lonardo, 2021; Treverton *et al*., 2018; Weissmann *et al*., 2021). Hybrid threats can be defined as the exploitation of existing vulnerabilities of an opponent state by state or non-state actors, using coordinated but diverse methods "while remaining below the threshold of formal warfare" (European Commission, 2021) which is a rising issue confronting state border authorities, and will be discussed in-depth further into this paper. Both traditional border management and cybersecurity are also heavily relevant to national sovereignty, from early readings (Sassen, 1996; Wu, 1996; Chayes & Chayes, 1998; Keohane, 2002) to the newer topic of digital sovereignty (Couture, & Toupin, 2019; Thumfart, 2021; Martins, Lidén & Jumbert, 2022), which merits a closer look.

Several perspectives of border management through the turn of the century concerning everything from smart borders to hybrid warfare raised concerns about the idea of digital globalization, although states in early twentieth century were ostensibly not yet interested in the idea of controlling sovereignty in cyberspace (Wu, 1996). Furthermore, many authors I have referenced in my research have written works in the past five years or so, and therefore, do not have significant overlap in their musings since they were all writing around the same time, but there has been an explosion of interest on the topic of cybersecurity as evidenced by the thousands of results received if too broad with one's wording in the library search engine. Some well-known historical authors do come up often in cybersecurity literature, such Keohane regarding his theory of sovereignty (which is subject to erosion by cyberspace), or Waltz' description of realism which focuses on survival, but these are theoretical applications as those authors of course could not say much about cyber topics directly. I hope that my research will help to bridge this gap between cybersecurity, border management and theoretical applications, and offer new directions for further exploration into the cloud as the fourth border type.

1.2 Central Question

I hope to demonstrate that the cloud is the fourth border type after land, sea and air. Border management agencies and cybersecurity networks all have the same goal of protecting national security from external threats. Threats which used to be purely physical are now leeching into the state via cyberspace. The cyber border may be as porous a cloud, but by definition of the threats being external, it is a border nonetheless. Given the shared objective, and border management's long history and therefore institutional memory in dealing with ever-evolving challenges, I would like to explore whether border management is equipped to take on the protection of the cloud border.

[1] In general terms, for example, most scholars would accept that Karl Marx is the founding father of Marxism, Morgenthau as the developer of Realism in international relations theory, etc.

1.3 Argument

Certainly, traditional border management alone will become increasingly less impactful for the maintenance of national sovereignty if it remains without heed to the threat of cyber interference, or if it attempts to confront hybrid threats at borders via physical and policy resistance only. That is not to say that physical border management will become obsolete, nor that its learned lessons cannot be adapted to the present. Physical borders remain the heart of a state's existence, and historically, there is much to be learned from them. However, the protection thereof is no longer limited to the physical world. I therefore firmly believe there are synergies to be identified in the overlap of physical and cyber borders which could enhance national security.

To defend itself in the cloud, a state can use some of the tried and true aspects of traditional border management. For example, border guards are more or less tasked with routinely checking every single border user at every single border crossing point of the country - daily, monthly, annually, on round-the-clock shiftwork, from border posts, on the ground, from inside a booth, office or airport, rain or shine, in war or peace. However, not every piece of border is an official border crossing point, as it would be impossible in most cases to set up along the entire length. Where border guards cannot be present are fences, cameras, patrolling officers or natural barriers in the form of difficult terrain or water, or at the very least, an agreement with the neighbour. It's not a perfect system, but it has worked well enough for hundreds of years to become the general minimum standard of state demarcation. Cybersecurity, similarly, is often fraught with the concern about the sheer level of data that must be processed in order to safeguard against threats, and it is called impossible in many circles. However, a 'good enough' approach could be systematically developed, not unlike the routine scrutiny of the border guard mandate.

My argument is therefore that not only is cybersecurity approachable as a border issue, but that border management is capable of taking on these external threats at the cloud border. Furthermore, BM's pre-existing strategies and policies are the best suited to do so, thanks to its institutional memory and history of managing external threats on a daily, even mundane, basis.

1.4 Scope and Method

My thesis will be largely focused on border management of the European Union's external borders, as well as looking at related policies of individual European countries where relevant, and reference ongoing cybersecurity actions of other high-income industrial countries (in the past referred to as "the first-world", but to avoid any offense of the term I opt for the former) for comparisons or general understanding. Here it should be noted that *internal* national cybercrime is not the focus of this thesis, which is typically under the umbrella of law enforcement agencies (LEAs) or Intelligence. The more interesting aspect for my argument is the protection of the state (or Union) from external cyber threats. Sources will be mainly sought from 2014/2015 onwards, as the era of the so-called migration crisis in the EU, as well as the impending Trump election in the US, and thus the beginning of widespread conversation in the Anglosphere about malicious interference through cyberspace.

The thesis will present a medley of existing political theories to examine whether border management and cybersecurity can fit together under a theoretical lens. Equally, I will look at several existing systems in EU, such as the Schengen Aquis, Integrated Border Management and the General Data Protection Regulation (GDPR), which are already dealing with both topics in different ways. Here I will also address existing challenges such as hybrid threats, irregular migration flows and the cooperation of the private sector, as well as offer recommendations for how to better confront them.

A case study of the Belarussian migration crisis in 2021 will be made, because as a third country that shares its border with three EU states (Poland, Latvia, Lithuania), its actions can and have had severe consequences on the operations at the EU external borders, which has led the EU to

make policy decisions for the EU as a whole. The case study will evaluate the failures of the cybersecurity measures that were in place at the time and their outcomes, and how those could have worked more preventatively in support of the overwhelmed border management systems.

The study will be approached with a qualitative research design as a simplified content analysis, which links source material together using common themes and search terms and summarizing their research, using primary and secondary sources. Causal inference is then used rather than distinct variables, in order to consolidate the overarching findings and infer new possibilities. The purpose of the review of the resources is to synthesize evidence that includes challenges, opportunities, and implications for policy and practice. Using Kumar's approach for a holistic research study design, as well as a case study (Kumar, 2014, p.123-125), I will examine secondary source data, identifying and analyzing emerging themes from the published research literature. The research will be based on existing literature from peer-reviewed sources, but also take into account news stories about national security issues from external actors, and publications by governments and think tanks about emerging trends in cyberspace and virtual cross-border threats.

The sourcing of relevant literature is conducted via a methodological approach using specific search terms and setting the publication date to filter out works prior to 2014, except in regards to historical reference (like the rise of the internet and emerging concerns and traditional methods of border management) or theoretical frameworks. I will also source from primary sources of central administrations, such as government publications on policy or funding, international organizations, and news of relevant events and public reactions. In respect to the confidentiality of my professional role, I shall only use sources that are publicly available, and the views represented in this paper are mine alone. I acknowledge my bias as a civil servant in border management, and note that when studying one's own profession, being close to the study topic and having insider knowledge is unavoidable. What is important is to make the researcher worldview clear, and to acknowledge that there is an impact on the research from being a member of the profession being studied. I intend to enhance my objectivity by consistently questioning myself and my findings, considering both sides of my research, and only consulting valid, peer-reviewed sources.

Finally, the paper will conclude with making policy recommendations for practical implementation of the protection of the cloud border.

In terms of limitations, there are limits to what this modality of research can unearth, given it is a study of existing sources, and furthermore as mentioned there is a paucity of scholarly works on the "fourth" aspect of border management. Certainly further research could incorporate primary investigation and resulting sources to further enhance understanding of the results of my research here.

Chapter 2 – The Theoretical Framework

This chapter will examine existing political theories or discussions as they relate to cybersecurity as a tool for state protection, in addition to the mandate of traditional border management, in attempt to synthesize the theoretical tools available to merge these topics into cloud border protection. I will consider theoretical frameworks that can be applied to cybersecurity in relation to border management, the concept of hybrid threats, and the political debate concerning online anonymity.

2.1 Cybersecurity

Political science, with all of its concepts and theories, has a long and well-catalogued, and oft-debated history (to its merit). There are countless articles and studies relating to the concept of power, economy, democracy and worldviews. Perhaps a few founders of political theory can be agreed upon: Plato, Aristotle, Machiavelli, Hobbes, Adam Smith, Karl Marx, Kant, to name a few, that are instantly recognizable and generally agreed to have been very influential in the field of political and social science. This rich history is not yet established in the field of cybersecurity.

There is very little overlap in sourcing by cybersecurity authors when it comes to strategic national planning for cyberspace and security. Many of my sources are recent and as such, the interconnectedness of peer citations is low. It is difficult therefore to grasp overarching, differing schools of thought in the context of cybersecurity. Instead, these newly-minted cybersecurity authors are doing the groundwork of comparing national current events and policy against technical studies to predict or draw parallels between potential outcomes. If I am lucky, one of the sources I rely on in this thesis will emerge as a great in the coming years.

I have, however, identified a few base-models in computer science that were written in a technical, usually corporate-minded context, which later scholars projected into political cyber governance discussions. For example, Boeke & Broeders (2018), accomplished authors in cyber governance/cyber security topics, extrapolated the theory of Provan & Kenis (2008) on the three modes of network governance (democratic/participant-led, lead/hierarchical, or network/external) and their effectiveness, to provide a structured guideline to different EU country government approaches of network governance especially in relation to crisis response. Although Boeke & Broeders do not make a value judgement on which mode is most effective, as they observe that each example is too new and too ‘under construction’ to “transpose best practices from one system to the other without considering the broader context,” (2018, p.13) they are able to expand on the network modes theory to introduce two further questions whose answers dictate governmental responses to cyber crises: whether the computer emergency response teams (CERTS) operate within or independently from central intelligence, and whether response actions are concentrated in one branch of government, or spread amongst branches where relevant (Boeke & Broeders, 2018, p.13). Kapucu & Hu go on to cite Provan & Kenis’ same work in their study of the US pandemic response that a global and large-scale incident cannot be addressed functionally well with a hierarchical network model. They propose instead that “such networks need to be governed by multiple lead organizations within a hybrid governance structure” (2022, p.790). In light of these works, it would not be amiss to replace “pandemic” with “cyber threats”, as both are globally reaching and require coordinated cross-border response networks to effectively combat the threat. Boeke & Broeders’ contribution also highlights faster and more precise information-sharing when the response team is involved in the intelligence community. In the European Union, the International Criminal Police Organization (Interpol) is working closely with the European Border and Coast Guard Agency (Frontex) to provide real-time access to police databases which helps their shared goal of combating transnational crime through effective border security (Interpol, 2017). In this way, cybersecurity should be approached as a border management topic because BM is already entrenched in the intelligence community and relies on

strong, cooperative lead-networks to quickly and effectively spread information to generate fast responses. Boeke & Broeders (2018, p.454) purport that cyber defense is a team sport, and so is border management.

George Christou (2016) is an oft-cited author in recent works in his textbook about cybersecurity in the EU, which delves into the EU's growth as a pioneer in civilian cybersecurity but that there is much more work to do to reach true resilience. He is frequently mentioned in further studies in cybersecurity, resilience and the EU (Brandão & Camisão, 2021, p.18; Terpan & Saurugger, 2021, p.1337; Carrapico & Barrinha, 2017, p.7) as a jumping-off point of trusted background information off of which to build their arguments, reaching into the Commission's role, policy building from crisis response, and the legitimacy of the EU as a security actor (respectively). Christou is among many to use the term "borderless" in reference to cyberspace, such as when he suggests that "the global interconnectedness of the Internet ecosystem means that threats can emanate from any source around the world, which in turn requires solutions and policies that are borderless." (2016, p.35) and yet later contradicts himself when he writes, "sharing information across borders is a pre-requisite for security as resilience – and a norm that all participants involved in cybersecurity should adopt and operationalize in order to ensure effective reaction and response to cyber incidents" (2016, p.56). If cross-border solutions in and of themselves can ensure effective responses, then why should proposed policies and solutions be borderless? Tailor-made responses and flexible partnerships (2016, p.114), albeit based on "a common terminology" (2016, p.118) are crucial to building the cybersecurity resilience that the EU needs, which requires a greater reliance on complex cross border nuance.

Andreas (2003, p.78) discusses border control just after the turn of the twenty-first century, in which the emphasis was shifting from territorializing the state, to a greater focus on policing what he called CTAs: clandestine transnational actors ("non-state actors who operate across national borders in violation of state laws"). At a time of increasing globalization, new technologies and database systems facilitated smoother passage of trade and legitimate passenger flow. Andreas marked the observation that border management was less and less about military defense of borders and moreso about "constructing a more expansive policing and surveillance apparatus that increasingly reached beyond physical borders" (2003, p.107). He rejected both the realist view that borders are of primary significance to the military, but also the globalist view that borders were becoming irrelevant.

The rise of the internet created new vulnerabilities through cloud technology and cyberspace to national security. This evolution already sparked concern among scholars in the late 90s and early 2000s, but on the more specific topic of the necessity of cybersecurity of the nation state, I must defer to works from 2015 or later, as earlier articles cannot encompass the extreme changes the world has undergone since the explosion of the internet affecting global politics. De Spiegeleire, Jans & Rujan describe transnational terrorism through cyberattacks as a "terrifying game of whack-a-mole" (2017, p.10), as the entire world becomes more connected, it also becomes more vulnerable. Jupillat discusses another angle, which is the potential damage that could arise should a state invoke retaliatory self-defense (as pre-emptive self-defense is too broad an undertaking for singular attacks, when resilience is not possible) in response to external, non-state cyberattacks, and is adamant that international cooperation must prevail to override the actions of a rogue citizen to maintain peaceful relations with the injured state (2015, p.129). However, five years following Jupillat's warning, countries are beginning to "tighten their internet borders" according to Goel, in order to better control vulnerability to cyberattacks (2020, p.73). Goel proposes methods to avoid "Balkanization" of the internet, as well as considerations for the balance between security and freedom of innovation but that which, he concedes, cannot thrive in a chaotic and criminal environment regardless. Sargana, Sargana & Anns (2020, p.332), echoing Goel, predict that the next age of insecurity will stem from cyber-weapons, and found that cybersecurity debates in international forums are quickly reduced to

geopolitical discussions, which lends credence to my theory that cybersecurity is indeed a border's issue – and not "borderless" by any means.

2.2 Hybrid Threats

The terms 'hybrid threats' and 'hybrid warfare' tend to be used interchangeably, because the tactics are used in the same sense as 'physiological warfare' in that they are relentless and have a certain plausible deniability attached to them (Häggström, 2021, p.132). This makes the use of 'warfare' confusing because war is associated with brutal, actual combat. Hence, 'threats' is a better signifier of what the tactics really are, which is a barrage of combined attempts at exploiting the enemy target, while operating under the threshold of war, carried out by state or non-state actors (European Commission, 2016). Frank Hoffman wrote in observation of hybrid warfare that "the adversary will most likely present unique combinational or hybrid threats specifically targeting vulnerabilities. Instead of separate challengers with fundamentally different approaches (conventional, irregular, or terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously" (2009, p.35). Weissmann *et al.* advocate for a military role in countering hybrid threats (2021, p.70). However, they write that "vulnerabilities tend to exist precisely in the border areas between sectors and levels, and this is what the opponent will target" (2021, p.25) which in my view necessitates involvement of border authorities, albeit with strong communication channels between all relevant sectors and levels.

Types of hybrid tactics frequently seen in modern day that involve a cyber component may present in the form of the instrumentalization of irregular migration (see the case study of Belarus below), the use of economic coercion, foreign information manipulation and interference through disinformation and direct interference in elections and political processes (as detailed in the Strategic Compass of the EU by the General Secretariat of the Council, 2021), to name a few. These could be further combined with traditional tactics such as propaganda, staging false protests, forming military camps at borders in peacetime, claiming weak attacks or invasions as accidental, etc. (Treverton *et al*, 2018, p.60). Although the idea of multiple forms of warfare at once is nothing new, the idea that the interconnectedness of citizens invites a constant security threat exactly through that interconnectivity is what makes this era of hybrid threats something new. Lonardo assesses which tools the EU has at its disposal to counter hybrid threats (mainly legal and regulatory), given that security is typically left to the individual member state, and notes the EU largely only becomes involved when a cross-border threat is detected – but that given the continual nature of hybrid security threats, it warrants continual involvement (2021, p.1077). In some ways a common threat brings greater unity in the EU as responding to external threats increases interdependence, information sharing and cooperation among member states, just as "border security practices respond to [threats] with risk analysis, information exchange, and interagency cooperation" (Lindblom & Castren, 2021, p.90), in which synergies in the security sector, cyber and physical, can be examined.

2.3 Legality and Anonymity

An intriguing question about detecting cybercriminals outside state borders is what to do with them once identified? Outside of the state, there is no jurisdiction over a criminal. The short answer is extradition. Mann *et al*. (2018, p.22) discuss the legal challenges that surround law enforcement outside of the territory especially in regards to where the sentencing should be determined – in the state of the source of harm, or in the victim state? If the origin state is unable or unwilling to apprehend the individual, LEAs can indict or ban or place whatever pertinent sanctions possible on the individual, who would then be flagged if trying to enter the jurisdiction at any point in the future.

This is obvious at border crossing points, but could be carried further to the cloud. IP[2] address data – which is albeit easily spoofed with a VPN[3] – or otherwise future developments towards creating unique online footprint identifiers for persons of interest, could create an alert for if/when the person is attempting to re-enter the victim state's cyberspace, whether to commit further crime or not, exactly like how the person would be apprehended if attempting to cross a physical border, on holiday years later by mistake, or not. While physical or cyber bans from the victim state's territory may not be a satisfying punishment to LEAs seeking to carry out justice, it is a start, and also creates a last resort consequence for individuals of states who are unwilling or unable to extradite their citizen. In that sense, is a VPN all that different from a faked identity being used to cross into a state using fraudulent documents? VPNs are currently used quite freely for the purpose of online privacy and network freedom, whereas faked passports are almost always a criminal offence. From the perspective of a cloud border, the virtual equivalent of document fraud may begin to resemble IP fraud (which is basically the whole point of a VPN), which would have a significantly negative impact on the anonymity of the internet. Here especially the topic veers into more technical territory and I invite further research from computer scientists to answer my question as it invokes the questioning of a right that exists online (anonymity) which wholly does not exist at borders. I expect this question would be a sticking point in the larger debate of the regulation of the internet, especially if merged with border topics.

[2] Internet Protocol (IP) Address is a unique identifier attached to an internet user's online activity (who is not using encryption methods).

[3] Virtual Private Network: an encrypted online connection that obscures the user's internet activity or circumvents geo-locked censorship. Ensures greater privacy and anonymity to the user, as well as increasing accessibility to blocked data geographically. (Gillis, 2022)

Chapter 3 – Border Management Policy

Whereas the topic of cybersecurity is still not fully situated in political theory, border management has a much deeper history of theory, change and debate. Through the lens of addressing several current challenges in border security, namely irregular migration and the Schengen crisis, this chapter will look at applicable theories and existing policy avenues, e.g. integrated border management, involvement of the private sector, and the General Data Protection Regulation, and their outcomes so far. Lastly, this chapter will also look at the cloud border through the theoretical prism of the debate surrounding security versus right to privacy, and sovereignty of the state in a digitalizing world.

3.1 Irregular Migration

It is inadequate to discuss borders without mentioning the practical uses such as migration, which is especially a divisive topic in the EU today. On the topic of realism and globalism in regards to borders, Meyers places these theories in the context of immigration policy. The realist view of the state as a self-interested, rational and solitary actor with the key motivation of survival (Waltz, 1990, p.31) tends to view economic politics (under which immigration commonly falls) as secondary to security (Gilpen, 1984, p.290-291). State military or security actions *can* cause high traffic flows or influence immigration policy, which was especially apparent during the world wars (to prop up/repopulate the population) or the Cold War (to show goodwill towards those fleeing communism) (Meyers, 2000, p.1264), but by the year 2000, we had not quite yet witnessed the opposite, wherein the immigration policy triggered alerts for national security. A more recent analysis ties in the inward-turning impact that the pandemic has had on the world as a return to "stone age realism," especially in terms of national security and the shuttering of borders, but that this shift had already been developing since at least 2016 (Roloff, 2020, p.27). The timeframe can of course be attributed to the attitudes towards migrants following the heavy influx during the migration crisis of 2015, which slowly soured Europe's globalist and humanitarian outlook, while the pandemic hammered the final nail into that coffin, according to Roloff. However, he concedes that when the EU member states shut down all borders, halting trade and stranding travellers, without coordination or respect to their commitments as EU members, the EU Commission stepped forward "for the first time reminding the EU member states of their obligations" (2020, p.30). Although early in the pandemic, Roloff was able to predict the survival of EU solidarity in crisis, but warned that it must continue on the basis of its former postmodern paradigm of globalism in order to remain a strong contender in the world order as a normative and transformative power (2020, p.35).

Returning to Meyers' application of globalism in immigration policy, there is a school of thought that while exclusive territoriality may be undermined by economic globalization, that sovereignty itself may have transformed and no longer require the demarcations of militaries past. If trade and ideas should easily flow through borders, then the mobility of people can likely not be stemmed (Meyers, 2000, p.1267). Sassen points out the hypocrisy, suggesting that states "must reconcile the conflicting requirements of border-free economies and border controls to keep immigrants out" (1996, p.93). The evolution of these ideas peaked with the migration crisis of 2015 and its aftermath, in which over five million refugees entered Europe by the end of 2016 (UNHCR, 2021), by which time the EU was beginning to take back its open border narrative, and took the first steps towards building its own border guard service at external borders ('Regulation 2016/1624/EU,' 2016) – a disastrous rollout, to be sure (Liboreiro, 2021), which even now has not fully come to fruition, but that signaled the EU's changing intentions towards migrants nonetheless (Bruycker, 2016). Frontex has committed to hire and train ten thousand standing corps officers for EU external borders by 2027 (Europarl, 2019) which means that migration has possibly been reclassified from an economic issue to a security one, and that border security is being partially handed over to a

centralized agency of the EU. As Andreas (2003) predicted, neither realism nor globalism gets borders quite right in the twenty-first century.

In the current climate, in which the pandemic has faded in relevance while the war in Ukraine following the Russian invasion rages on and economic inflation runs rampant, the EU has taken two stances: first, the doors are once again flung wide, for Ukrainian refuges this time, and there is very little bitterness in their reception, despite the way the migration crisis tapered off "last time" in which the Europeans' welcome, sadly, tended to have worn out for refugees from the Global South (Ramji-Nogales, 2022, p.150). Secondly, the EU has taken on a strong military stance, sending billions of Euros worth of weapons and support to Ukraine (EC, 2022), expediting its own military forces' creation and encouraging military training in individual member states, the fast-track consideration of allowing new members to join NATO, and the recommitment to the NATO protocol in which all members stand ready to defend if Russia (or anyone) provokes another NATO member (Tardy, 2022, p15). Although we are probably no longer living in a time period that history books will refer to as 'peaceful', it has been interesting to witness a marginal return to globalism, although it looks slightly different now, perhaps a little more wary. What was once humanitarian goals for the sake of promoting normative western values (Keukeleire & MacNaughtan, 2008, p.137) is replaced by targeted development with the goal of convincing migrants to stay, or at least stop short of the EU's external borders (Fröhlich & Müller-Funk, 2020, p.4). What were once cooperative international organizations based on postwar strategic alliances are now vital brothers in arms. It is using liberal methods of combined organization for realist security goals of military survival and greater-good self-interest, because we are too interconnected, too intertwined, to go back even if we wanted to – and it's starting to seem like we wish we could. It would be far too costly and disadvantageous to disentangle the state from cross-border and online opportunity. But if this guarded globalism is the new norm, then cyber border management can be approached in a similar fashion: *careful* security at borders while facilitating *careful* trade and migration through new technologies.

3.2 The Schengen Acquis and crisis theory

Next it is important to consider the role of Schengen in EU external border management, in the context of harnessing a crisis for beneficial political gains. Winston Churchill coined the phrase in World War II, "Never let a good crisis go to waste," but unfortunately, Blumenau explains how the Schengen crisis deteriorated integration between the border-free agreement area, and it still has not recovered fully (2018, p.476). The Schengen acquis is an agreement between twenty-six European countries to abolish internal border controls, grant visa-free travel and harmonize security at external entry points (schengenvisainfo, 2022). A key sticking point in Schengen's operation has been the Dublin Agreement that dictates that asylum seekers must be processed at the first point of entry to the EU, which has caused friction since the development of increased migration flows via sea-crossings, putting undue pressure on Mediterranean coastal member states. Walters, a liberal scholar, presents the role and limitations of the Schengen borders through the presentation of three genealogies of the responsibility: the geopolitical border, the national border, and the biopolitical border (2002, p.561) and considers the question of sovereignty for the states within the agreement (2002, p.577). He claims that "the linear border enclosing its national territory is a historical, not an eternal phenomenon" (2002, p.577). This was the globalist optimism surrounding the perceived success of Schengen at the time, and it an interesting historical snapshot, also in the case where he questions how international airports can represent an external border "from the inside" (2002, p.577). Blair, on the other hand, analyzes Schengen and EU border policies in relation to the 2015 migration crisis. He describes how irregular migrants and asylum seekers took advantage of the open-border Schengen system to enter Europe by crossing the Mediterranean Sea to the southern member states like Italy and Spain, with goals to continue to more resource-rich and welcoming states like Germany (2016, p.20). This time period signified a crisis for the Schengen acquis as members felt disproportionately burdened, threatened to leave, or even took measures like building fences to quell the flows of migrants into their own borders (2016, p.60). The actual enforcement of the 'single external border' goal was left to

the responsibility of the individual member states, who were unprepared for the massive influx of refugees. Meanwhile the Dublin agreement encouraged asylum-shopping in the Schengen zone and rules were applied unevenly by different members (Schimmelfennig, 2018, p.11). The same author concludes that the Schengen crisis was not able to harness the common threat into greater inclusion and solidarity between members going forward. Basically, a good crisis gone to waste. Coon believes Schengen is worth saving, but only if it bends with today's challenges to introduce necessary reforms (2021, p.19).

Cybersecurity was low on the priority list during the migration and Schengen crises, but a higher integration of systems, databases and info-sharing may have alleviated some of the challenges. At the same time, privacy was (and is) still a highly exploited aspect of online presence, especially pre-dating the General Data Protection Regulation (GDPR), which I will discuss shortly, and without proper training and ethics among officials, may not have been properly executed. As migration flows have lessened since the crisis, but picked back up following the end of pandemic shutdowns, this is a challenge that agencies tasked with EU external borders will need to address.

3.3 Integrated Border Management

Current methods of border management in the EU at external borders focus on the protection of land, sea and air borders, but are developing greater focus on surveillance, tracking, profiling and prevention, in order to systematically prevent abuses, rather than relying on the case-by-case reactions at the discretion of a human border guard or customs agent. This enables faster processing for bona-fide travelers and business trade, as border management carries the dual role of preventing crime but encouraging economic growth and international partnerships (Gerstein *et al*., 2015). With goals on opposing sides of the spectrum, unlike agencies purely focused on security, border management institutions must strike a balance in all approaches because a closed border will harm the state just as much as a fully open one, as discussed by Pluim & Hoffman (2015) in a working paper put out by the international migration organization ICMPD.

The same is often debated in the topic of cybersecurity, as discussed above, in which security should not stifle innovation and creativity that the internet enables. This dual-role of border management was a hot topic at the turn of the century, as economies became more globalized but terrorism was on the rise. The EU had just developed its first iteration of the integrated border management strategy in 2002, which has become a highly influential topic in the border management world. The concept of integrated border management (IBM), as explained by Wagner (2021, p.425) and promoted by EU-funded institutions, is already in place as an EU best practice (EC, 2016), and promotes cooperation and coordination between border agencies, among nations and state authorities, and across neighbouring borders.

IBM is aimed at increasing security at borders while leaving them open enough to capitalize on the rapidly globalizing economy. It is based on a three pillar approach that enables intra-service cooperation (between agencies present at the border), inter-agency cooperation (between border actors and other levels or branches of government, including LEA and Intelligence agencies), and international cooperation (between neighbours or other interested states or organizations) (ICMPD, 2022). In today's practice, IBM is a holistic approach to let coordination between border actors become a standard, facilitate real-time information-sharing, increase trust between actors, share best practices, reduce costs of duplicating services (such as the single window approach in which the same checks are not performed at multiple points of a BCP), and thereby overall strengthens border management and security for all partners. If state border agencies are already sharing information this way, there is surely room to expand into cybersecurity domains, which also necessitates an inclination for info-sharing.

Border management is at times wrongly accused of existing solely to create stops, blockages, and pursue security goals above all else. This is also a common complaint about cybersecurity. What IBM strives for is to strike this very delicate balance between border security, while also letting borders be a place of opportunity. Tourists and migrants bring prospect and prosperity, as does trade, investment, and agriculture. Refugees and asylum seekers, in the EU, may also exercise their human right to seek refuge in the next safe country, and border agencies may not stop them without due cause. IBM makes way for these legitimate passages to take place, as quickly as possible, so as not to hinder the opportunity that they bring (Polner, 2011, p.67). Likewise, cyberspace is a place for innovation, diversity, linked economies, and development, and cybersecurity efforts must not squash these worthwhile pursuits, but must neither allow a free-for-all space where criminality rules. In that sense, cybersecurity can learn a lot from the twenty-plus-year history of EU integrated border management.

3.4 Private Sector Involvement

On the topic of states securing national cyberspace, Weiss & Jankauskas analyzed cybersecurity policies across fifteen different states and found that governments are more likely to outsource control to third parties in response to attacks (while maintaining control of the hierarchy), but orchestrate internal responses in response to recognized threats or weaknesses (2018, pp.271-272). This raises several issues, first that it implies the government is lacking competence in rapidly developing technologies and therefore must outsource, which secondly is expensive for the taxpayer, and most importantly, leaves the state in a weakened position to respond to direct attacks due to the lack of internal expertise and capacity. Of course, it is normal for governments to outsource for expertise, but there are surely better ways to go about it. If there is money to be spent on private expertise, it ought to be preventatively done on an ongoing basis, rather than reactionarily (which may cost more on the budget upfront, but is certainly cheaper than the damage control that follows an attack and hasty development of a patch to place over the discovered vulnerability). However, one challenge that cybersecurity will face differently than the border sector is the willing support of the private sector in general (aside from the outsourced contractors naturally). Due to the high involvement of private actors as stakeholders, namely businesses transacting international trade, traditional border management reform was able to be shaped by stakeholder concerns with the common goal of trade facilitation without losing control of the security situation, so states were able to capitalize on industry expertise through ad-hoc consultation, collaboration and contracting with the private sector (Grainger, 2010, p157). Unfortunately, cybersecurity and sharing information is less in the financial interest of corporations this time, not to mention that the biggest players are not based on EU soil or particularly concerned with foreign nations' security (nor their own, to be fair), and individuals could potentially even be sued for leaking corporate trade secrets.[4] The government will need to be a little more aggressive in order to enforce the same support as was given to border management reform, and one option would be to combine the two issues under the cloud border in order to preserve perhaps a small amount of the goodwill afforded in previous trade negotiations.

In the same vein, the EU's proposal for the Joint Cyber Unit (JCU) is not a bad one, which aims to equally involve "Member States and relevant EU institutions, bodies and agencies, including

[4] See: the case of whistleblower Frances Haugen who faces legal repercussions for leaking Facebook's internal documents to a US Commission and the Wall Street Journal, that revealed Facebook actively prioritizing profits over the safety of its consumers (Pelley, 2021).

ENISA[5], CERT-EU[6] and Europol[7], to promote an incremental and inclusive approach [to cybersecurity], in full respect of competences and mandates of all those involved" (EC, 2020, p.14). However, taking the aforementioned criticism into account about the lack of protocol for involvement of the private sector – the vast owner of cyber technology and data collections (Dempsey & Flint, 2004, p.1466) – and no overarching implementing authority, the initiative is probably doomed to fade into obscurity as those same institutions develop their own, better solutions in parallel for their own priorities. Government *likes* hierarchy. It should not be afraid to delegate proper levels of authority and differentiate tasks between different agencies and ministries, and guidance for including the private sector. I agree with the 2020 Cybersecurity Strategy mentioned in the forthcoming case study that suggests there is little sense in building a new agency altogether, as it would just create yet another division without institutional memory or experience, and leave them to fend for their own silo. However, I believe that the answer does not lie with *no* common authority, rather that the institution that will take on a managerial role in the JCU or similar future initiatives should be one with experience in merging cross-sectoral directorates and business regulation.

3.5 General Data Protection Regulation (GDPR)

The European Union has already proven itself willing to advocate in uncharted policy such as the General Data Protection Regulation (GDPR), "the toughest privacy and security law in the world" for safeguarding privacy of EU citizens against foreign collection or targeting of private data, enacted in 2018 (Wolford, 2022). The European Council on Foreign Relations released an essay collection on the topic of Europe's role in the digital market in what was formerly the US-China dichotomy. A few interesting conclusions were noted, in particular, that democratic governments who value the balance of security and privacy are looking to the European model with more interest than that of the US or China (Puddephatt, 2020, p.23). However, that "referees do not win the game" Burwell and Propp (2021, p.1) expand on this notion by explaining that the EU's fate is to either be to redefine norms in cyberspace that will eventually permeate international cyberspaces, or to exist in its own protectionist cyberbubble. Veit discusses the challenges as learned under GDPR for enforcement, which particularly aligns this notion of losing relevance if the EU does not also promote its internet regulations abroad. He aspires to a faraway goal of a "global data protection framework" and refers to the GDPR as an example of "postnational governance", due to the transboundary interaction of networks that would entail the transnational governmental scope (Veit, 2022, pp.445-446). Veit would likely disagree with my claim that the cloud will constitute the next border, however, to this I respond that in reality, globalism as it existed in the turn of the century is diminishing as illustrated in the theoretical chapter of this thesis, and therefore the envisioned borderless world with harmonized digital frameworks, physical or in cyberspace, will never come to be. What *can* potentially be reached are internal or cross-border agreements such as this one, GDPR, that can apply political pressure on other states to follow the EU model by enforcing restrictions on data transfer if they do not adhere to the minimum standard of agreed regulations. The EU represents a large share of global trade and cutting off internet services for data transfers between unapproved countries would be painful, especially in certain import sectors and social media. If enough world powers introduce the regulations necessary to join such a partnership, smaller powers will be pressured to follow suit lest they get left behind entirely. However, this is different from the idea of a single framework, which implies a central authority. I am therefore not convinced to accept his term 'postnational' governance. The individual state is at the heart of world order and cyberspace does not change that. In any case,

[5] European Union Agency for Cybersecurity is an agency of the European Commission that oversees cybersecurity in the EU.
[6] Computer Security Incident Response Team of all the EU institutions, bodies and agencies is a cyberdefense entity administratively positioned under the Directorate for Informatics of the European Commission.
[7] European Union Agency for Law Enforcement Cooperation, a supranational LEA for cross border criminal investigations in the EU.

the GDPR is the best example so far of cyber-governed borders, as it does not aim to surveil outside its jurisdiction, merely to stop-and-search third parties from entering the Euro-cybersphere without adhering to European data law standards. This is proof that the same principle could be applied in other areas of external online threats.

3.5 The Theoretical Prism

This thesis would be incomplete without taking a look at the current prism of debate that affects this topic. Border management and cybersecurity share the dilemma of how to balance human rights of privacy and freedom with the right of the state to protect. Going further, there is also the question of state sovereignty as a whole – border management is an expression of sovereignty but cyberspace is eroding it. How do we reconcile these diverging outcomes?

Let's start with the political dilemma in this topic which affects both border management and cybersecurity in a similar fashion. There must be a balance of surveillance and security technology versus right to freedoms and democracy. Since 9/11 there has been considerable increase, and resulting backlash, against invasive surveillance methods at borders, such as summarized more recently by Sadik & Kaya in their assessment of increasingly restrictive migration policy which seems to be motivated by security concerns. They found that although the "EU's centralized databases are not only to manage asylum or migration at the borders anymore" they recognize the necessary evil the databases present for safeguarding "internal security, to counter terrorism, and to combat organized crime" (2020, p.159). This tends to capture the general mood in the EU regarding security – people don't like to be tracked, but consent to reasonable border controls if it supports the security of their homes and lives.

But even more backlash has come regarding invasive data collection and targeting following the Covid-19 pandemic. General debate about how governments should have responded to the viral threat exposed how vulnerable democracies are to disinformation, yet how fiercely they oppose censorship, as related by Speier (2021, p.1), especially in the US, but also in Europe. Governments must proceed extremely carefully when it comes to regulation of information. Contact tracing, enforced isolation, or even outside of direct governmental intervention, within internet culture real life backlash and consequences came to individuals acting outside of the acceptable narrative by their peers. This may have convinced citizens on either side of the debates that such personal consequences deriving from their whole lives being searchable and accountable online may not be a good thing. Heldt suggests the way forward relies on companies to implement better oversight (2019, p.356), while Siripurapu and Merrow lay more responsibility on policymakers (2021, p.2). Certainly, corporations are not prone to choosing what's right for their consumers if it means generating fewer profits. In that case, it falls to government to regulate them. This proves difficult in the EU case, as the most popular platforms are based in the US and therefore EU regulators cannot force them to adopt EU policy. The EU's best bargaining chip here is to threaten sanctions or altogether pulling access out of EU markets, which, to its credit, has worked decently so far, as reported by the New York Times (Satariano, 2021), but also faces heavy criticisms by proponents of free speech, such as in an article by FP (2022), which claims that the EU regulations will "cause serious collateral damage to online free speech in Europe". But to come back to the balance of privacy and security, Goel cautions: "In the absence of effective and verifiable norms, we should expect to see a continued tightening of Internet borders and increased surveillance of the Internet and social media" "as countries will not feel secure" (2020, p.85) and warns of the development of a classic East-West divide as some proceed with heightened cybersecurity while others maintain the free-for-all status quo. If we do not avert this trend, we will lose the advancements gained by interconnectivity in the first place (2020, p.85). Tighter internet borders while still encouraging "the free flow of information [but] protecting sensitive information" is the only way to achieve actual security in the cloud (2020, p.85).

Keohane offers the historical background of another argument, which has similarities with the dilemma presented above but is rooted in the concept of sovereignty, in that European sovereignties are increasingly perceived as "shared business" (Keohane, 2002, p. 744). The European Union "gave birth to the concept of external state sovereignty" (2002, p.761), and he praises the EU as a model of mutual interdependence, which gives "European states incentives to pool and limit their sovereignty in the interests of more sustained co-operation." This has also been controversial, not only from inside the EU but for the world order as a whole, not least because attempts to replicate its degree of close-knit institutionalization in other regions of the world were not successful (2002, p.755). However, the EU does allow for individual states to remain prominent actors on the global stage in their own right, which Chayes & Chayes (1995, p.26) call the 'new sovereignty'. How does this debate translate to today's concerns of digital sovereignty? First, note that digital sovereignty and technical sovereignty are often used in discourse interchangeably (Bellanova, Carrapico & Duez, 2022, p.349). Thumfart proposes that which hasn't changed; "in practice, sovereignty is primarily attached to territory" (2021, p.4). Barrinha & Christou take this idea and push it a step further; with their term Conceptual Delineation (2022, p.358). Sovereignty begets location, even if that location is intangible.

However, states are not only up against other states and non-state actors, but specifically, corporations. Hubert in a briefing of the EU Digital Markets Act describes the existing situation in which digital gatekeepers, i.e. market giants like Google, Facebook and Amazon, "control key channels of distribution" (2021, p.2) because of their large user bases, intermediary role between business and customers, and massive amounts of collected data, from personal to market engagement to competitor data. Heldt even makes the point that social media giants are starting "to adopt new structures that resemble administrative law—an uncommon development for non-state actors" (2019, p.336), which should raise the alarm for any government when speaking of sovereignty over its jurisdictions. Thanks to GDPR there have been limitations on what kind of and how much data these platforms can collect but many lawsuits and restriction processes are still ongoing. This removes the self-determination of sovereignty from hands of the state and forces it to be reactionary. Indeed, Martins, Lidén & Jumbert are pessimistic about any chance for the EU to gain total control over "digital sovereignty in the realm of border and migration governance" due to the reliance on the private sector and digital solutions such as AI outpacing human/analog ability to genuinely understand them (thereby "undermining human control" (2022, p.489)), as well as biases of individual member states and reliance on EU institutions like Frontex (2022, pp.489-490). In that sense, total control must not be the goal of digital sovereignty, but rather fair and unbiased regulation and building the capacity for strong cooperation among actors.

The "digitalization of EU borderwork" also plays into this topic, in the sense that modernizing borders with state-of-the-art technical means will help speed up processing times that were previously carried out by human checks. Now, border agents have the use of artificial intelligence (AI), infrared technology, scanners, document readers, x-ray systems and biometric data collection, to name a few. These technologies are usually developed by and purchased from the private sector. Their use has the advantage of perhaps removing human biases of individual border guards, but come with new concerns over systematic biases created within the algorithm, which would now be in the hands of corporations.[8] Here interoperability is important, so that these systems can communicate with each other, regardless of the manufacturer or member state it is used in, but this is largely dependent as well on the private sector's ability to do so. Paradoxically, Martins, Lidén & Jumbert argue that this need for automated communication erodes EU sovereignty in and of itself, despite the EU's goal for interoperability is to increase its digital sovereignty (2022, p.484). However, without the deep pockets of the private sector for these innovations in the first place, and real world

[8] Systems using AI to make decisions are often trained using images of Caucasian adult men, thereby creating bias against women, child and minority users who do not match the 'model'. This is slowly changing, but it is an issue that has greatly impacted early subjects of AI discrimination and persists as an issue today in many areas where AI technology is applied for decision making. (see: Crawford, 2016; Ntoutsi *et al*, 2020, etc).

applications at borders to uncover the flaws, borderwork digitalization would not be possible to the extent that is already in place. Integrated border management can play a role in this regard by overseeing these systems and ensuring human and agency-led cooperation, coordination and communication is taking place to flag further issues as they arise. The cloud border would be an added element to digitalized borderwork which would also have to be taken into consideration for confronting inherent and built-in biases.

Finally, Calderaro & Blumfelde discuss the EU's weakened position of reactionary sovereignty building by the EU and criticize the EU's ability to develop a forward thinking approach. They highlight the result of the EU's protectionist initiatives as impactful "on the monopoly of US digital service providers and Chinese tech companies in the European market only" (2022, p.417). However, this might not be a bad thing, depending on the goals of the EU. If it is to protect its citizens and their privacy, then protectionism is not incompatible with that goal. If the goal is to be a leader in the global approach to internet regulation, a strategically autonomous EU may project the model image that others will want to copy. On the other hand, if the goal is to forcibly disrupt current market trends in order to export its approach for a harmonized global digital framework, it will likely not meet instant success – if this is the route the EU wants to take, it will be fraught with concessions and compromises, which will in turn result on a softer stance on internal cybersecurity for itself. The European border cloud should instead continue on its path of regulation and cyberprotectionism if it is truly interested in protecting the data of its networks and trust that once they have built it, and ironed out the kinks, other democracies will follow.

Chapter 4 – Hybrid Threats: Belarussian Case Study

Chapter 2 of this paper focused on the introduction of cybersecurity theories and threats, while Chapter 3 gave a brief overview of the evolution of border management, to illustrate the point that BM can no longer function as the state guardian from external threats without added protection within the cloud. This chapter will present a case study where physical BM measures alone clearly failed in response to a migrant crisis at EU external borders that was born and multiplied within cyberspace. This chapter will examine what could have been done to better mitigate the crisis, and give recommendations for the development of policies (new and existing), and a roadmap for implementation.

4.1 Case Study

The EU placed Belarus under sanction following the suspicious landslide re-election of Alexander Lukashenko in August 2020, who at the time was frequently referred to as "Europe's last dictator" in the media. The sanctions followed violent crackdowns on the presidents dissenting opposition, including against Lukashenko personally. This dealt a reputational blow to the state and the president, in addition to the sanctions and restrictions. Given the great power imbalance, Lukashenko could not directly hit back at the EU. Instead, a more clever plan was hatched to get back at the EU. Belarusian President Lukashenko "appeared to orchestrate what was advertised as a novel form of coercion" (Nichols, 2022, p.1). The Guardian reported in 2021 that migrants of Syrian, Iraqi, and Afghan descent had bought "packages offered to them by travel agencies that appeared to be closely connected to the Belarusian authorities" to reach Poland, from which they planned to travel further inwards in the EU (Chulov & Tondo, 2021). Travel agencies and even embassies were colluding in this plot. First, visa applications were simplified in order to allow third country nationals from specific origins to apply and enter Minsk. This would make up part of the travel package paid. From Minsk, migrants would be connected with a smuggler over Facebook for a fee to take them to one of the EU borders, at first mainly Poland, but also Lithuania and Latvia. They were assured that the handlers were well connected to the Polish border guards who would wave them through. In reality, the smugglers would reach the border with their human cargo and start attempting to cut holes in the barbed wire fences. As European guards caught on, they began cracking down in violent pushbacks and the smugglers would flee, stranding the deceived migrants at the border. Worse still, many ended up in between the space between Belarus' border and the EU's, and Belarus would neither let them back through. The resulting humanitarian crisis from the migrants trapped without shelter in the northern winter climate, as well as violence experienced at the border or overcrowding of smuggler vehicles sparked international outrage, which was largely focused on the cruel European guards who did not let these people in, instead of at Belarus, who orchestrated the mess.

The affected EU border states declared a state of emergency and reinforced their borders with fences and stronger barriers (Euronews, 2021), while internal backlash escalated in Europe, in which activists held demonstrations and attempted to cut holes in the fences from the inside, while human rights groups condemned the border guards' violent reactions and unwillingness to help the stranded migrants. Meanwhile, Brussels tripled "the EU border management funds for Lithuania, Poland and Latvia to EUR 200 million overall [in 2021 and 2022]" using funding from the then-newly released Asylum, Migration and Integration Fund (AMIF 2021-2027, EUR 9.9 billion) in order to support more rapid asylum processing in the affected states (Von der Leyen, 2021). The EU was aware that they could not simply open the border to the migrants unchecked, because it would encourage more migrants to come, and signal to political foes that this is a successful tactic to sow chaos at Europe's borders. This crisis was dubbed a "hybrid attack", using the instrumentalization of migrants as a political weapon (Wesselink, 2022, p.5).

Hybrid warfare is a rising issue in the area of border management (Weissmann *et al*., 2021). In order to justify this case as hybrid warfare in BM, as discussed in the section above, there are many elements that flag this case as a hybrid threats study. The most obvious is the instrumentalization of the third country migrants (note that Belarus was not sending its *own* citizens into no-man's-land) in order to apply pressure at EU borders. Second, is the use of social media to spread disinformation about visa entry and one-way tickets to Europe. Third, which is yet unproven but highly likely, the extreme backlash that stemmed from within Europe may not have been entirely grassroots-led. There is a strong chance that Belarus, or sympathetic nations like Russia, infiltrated European cyberspaces to spread talking points in bad faith and encouraged protestors and dissenters to voice their concerns louder. That is not to say that no European could legitimately have come to these conclusions on their own – certainly, the border agencies are at fault for the inhumane treatment of the migrants – however, it would be extremely unsurprising to know that these conversations were not always held among legitimately concerned citizens only.

4.2 Recommendations and further exploration

Let's have a closer look at which cybersecurity policies were in place in the EU at the time of this case study. The new Cybersecurity Strategy, incepted in 2013 and built upon over the years, had last been updated in December of 2020. The policy document started with an overview of current cyber threats and concerns, and includes the following definite substantiation of insufficient policy already in place:

> *"The EU lacks collective situational awareness of cyber threats. This is because national authorities do not systematically gather and share information - such as that available from the private sector - which could help assess the state of cybersecurity in the EU.*"– High Representative of the Union for Foreign Affairs and Security Policy, 2020, p.3

The greatest ambition of the policy document is clearly marked as a subsection: THINKING GLOBAL, ACTING EUROPEAN. It outlines "three principal instruments –regulatory, investment and policy instruments" to offer methods of control and oversight in "(1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace" (2020, p.5). The policies then continued with suggested initiatives and reforms that could increase cybersecurity Union-wide, although it appears out of its depth somewhat in such a complex and technical field as cybersecurity. The recommendations seemed lacking in concrete steps, such as the proposal for a Joint Cyber Unit (JCU), which "would not be an additional, standalone body, nor would it affect the competences and powers of national cybersecurity authorities or EU participants" (2020, p.14), which sounds like yet another 'optional' platform for users to eventually ignore if not designed appropriately for the task it seeks to manage. As of now, I could not find information about the JCU's current status except for what it "should" accomplish, but not when or how. The overall strategy was criticized as lacking a roadmap to create a diverse ecosystem for collaboration between government and nonstate expertise (Lété, 2021, p.9), which is likely the reason why the JCU is not yet operational: such an ambitious platform needs to be state-of-the-art and user-friendly, two terms that do not usually come to mind when it comes to government infrastructure. Lack of funding and in-house expertise is common thread underlying much ineffective policy in all governments, not just in the EU. But with weak regulation over private sector (in other words: *effective*) data harnessing, any policy built upon fixing technological sovereignty challenges is likely dead in the water.

So what could have been the role of border management in this case if it had closer ties to cybersecurity? First, cloud Computer Emergency Response Teams (CERTs) tasked with monitoring migrant flows via keywords and specific routes may have been able to flag the travel agency

scammers while the scheme was in its infancy. As much of the planning began by using Facebook groups (which are not end-to-end encrypted, unlike Facebook's messenger function) to connect migrants with smugglers, this also could have been better monitored. By the time the migrants were reaching the Polish borders it was already too late, but even then, capacity and proper oversight could've been ramped up at the first sign of crowding in preparation for more, measured by border guard testimony as well as use of farther-ranging surveillance of the routes that were being taken, so that any further groups of migrants could at least be humanely received, if not sooner intercepted by other means (information campaigns aimed at countries of origin, greater sanctions on Belarus, participating countries and the travel agencies, etc), whereas the diverted support funding had to be used reactionarily for processing and to build crude last-minute blockades instead. The problem is that all of these red flags only became apparent in the hindsight investigation. Whether they were noticed at all by other governmental entities is unlikely, given the issue would be outside of the scope of the state's internal authorities, by merit of 1. No jurisdiction over third countries, whether Belarus or Iraq, etc. 2. It posed no major impact on internal law enforcement agencies given that the border guards are the first point of contact. 3. Intelligence tends to focus more on grand cases of crime and less on seemingly petty smuggling operations. 4. No regulations or agreements with Facebook to inform governments about these types of formations. In any case, since the route planning itself was fairly innocent (no different in the eyes of Facebook's AI filters from vacation tips or rideshare pages) it would have likely never been noticed by Facebook in the first place. If cloud border CERTs were placed under the border management authority to monitor against brewing situations such as these, an earlier response could be set up for impending suspicious or manmade migration flows such as this one.

Like cyber teams, border structures are also constantly facing new and changing realities, and due to their constant exposure to attempted criminal activity at their borders, they are constantly learning in real time about criminal behaviour and trends, down to the littlest signs. Their daily checking and patrolling work may seem at times monotonous when there is no detection of criminal activity, but this is just a part of what life is like on the front lines. Cybersecurity is generally lacking that aspect of mundane human patrolling. Yes, AI filters flag serious threats, but the threshold of most petty crime is not low enough to be picked up in such filters or else every person using a wrong word or making poor-taste joke would clog up the systems. Cloud border CERTs need to be deployed in daily, active roles to monitor potential cross-border criminal activity in the cloud. One of the defining issues in cyberattacks is the sheer volume of never-ending data, but like a physical border crossing point with human officers, the cloud warrants strategies for human intervention at low-threshold entry points as well.

In fact, many levels of agencies are already working together at BCPs with different specialty backgrounds just by virtue of the standard operation at borders, and therefore have a good handle on the type of coordination needed to prevent cyber-attacks and to disseminate information. At any usual BCP, one will find the following entities: Customs officers are trained in local legislation and recognizing dangerous or criminal goods, phytosanitary agents handle animal and agricultural import and were at the forefront of pandemic management, border guards are trained in human behaviour and the detection of document fraud, and all must be familiar with the databases and any kind of patrolling or surveilling equipment present, and may be flanked equally by units of police, military, coast guard, K9 units and handlers, social workers and non-governmental organizations, and may or may not have working relationships with their counterparts on the other side. It is also a best practice for border crossing points to be well integrated with the local border community in order to ensure their safety to not become casualties of border games, but to also remain aware of any suspicious goings-on. Part of a border agent's job is to stay on top of security developments and new tactics criminals are attempting and relate that information back to the central hierarchy. Rather than relying on central branches to assess and react to information given, would it not save time and money to station CERTs side by side with the border agencies, to see and hear the same whisperings and events through a

cyber-focused lens? Fahey mentions criticisms of the Council of Europe Convention on cybercrime "for its lack of provision for cross-border enforcement" (2014, p.3) and is supportive of the designation of CERT teams per member state to carry out cross border cooperation and info-sharing for critical cyber infrastructures (2014, p.7). Here I propose to take it a step further to create this new job profile at border crossing points, not only at the state level but also within the mobilizing Frontex standing corps fleet that [may] eventually act as border guards at the EU external border, the title of which I have already begun using above: Cloud Border CERTs. I envision cloud border CERTs as a fusion of a border guard and CERT agent, taking on the role of defending the cloud's entry and exit points.

I propose job creation physically amongst the border agencies at border crossing points, despite the fact that the nature of CERT work might sooner be placed at a central headquarters and closer to the servers and IT teams, for several key reasons. Christou provides a chart of the different roles and responsibilities of CERTs versus LEAs, which demonstrates that cultural differences in the nature of the job created difficulties in coordination and info-sharing between the two directorates (Christou, 2016, p.108, Table 5.2). In addition to the different functions, CERTs are also more likely to be younger, programmers or specialists in niche fields, college-studied and perhaps more naïve about the realities of the frontline. Whereas LEAs, much like border guards, tend to follow strict guidelines as taught in the military or police academy where they were trained, may be older with generational legacy in the LEA career, and can be more hardened to the human suffering they are privy to on a daily basis. It is of course generalizing, but summarizes some of the cultural divide in a nutshell. Despite this, their goals are exactly the same, and their general mechanisms differ only in the setting in which their work takes place. One of the best ways to overcome cultural differences is by spending time getting to know and trying to understand one another. A shared workplace, at the border, would help to bridge this gap. Not only for the social impact, but it is important for the holistic approach to build trust amongst units, to connect CERTs with the outcome of their work by spending time in the border communities and zones, and from a funding perspective, a decentralized approach to fieldwork is more attractive to investors and taxpayers.

4.3 Policy avenues

The EU is already constantly evaluating and updating its policies, which shows a willingness to adapt and push novel regulation. As Weissmann *et al*. explain, this approach "save[s] time and money while minimizing the impact on EU agencies by embedding [new] responsibilities into pre-existing strategies, agencies and institutions" (2021, p.50). This holistic form of approach certainly falls in line with the EU's normative values of information sharing and involving all actors in a way that enables trust and communication. However, this approach tends to suffer from the same drawbacks as the EU as a whole, in that with so many actors involved, it can be difficult to make concrete steps.

The Strategic Compass is the latest initiative for cyber control in the EU. It sets a very strong ambition to "act rapidly and robustly" to cyber threats, secure the cyber domain, invest in better technological capacities and innovations, and strengthen cooperation with partners with the goal of strengthening the security and defense policies of the EU by 2030 (2021, p.3). The compass was under development for years, but only released shortly after Russia's invasion of Ukraine and therefore greater public attention was placed on the defense aspect of the compass, whereas during its developmental stages the focus had been more on the cyber front. Because of this, critics called the policy already obsolete (Witney, 2022) because the meager military proposals were formed in peacetime and likely would have even been controversial if released just a few months' sooner, before the war. For that reason, in the new reality of an unstable Europe, military defense and cybersecurity should be decoupled. They are indeed closely linked topics, but so independently volatile that they cannot risk to overshadow each other, as what happened with the compass. The EU is not a leader in

military power nor is it currently seeking to be. It is however a leader in integrated border management, and seeks to spread its normative values for a secure but fair online experience to its citizens, and become a model in internet regulation globally. For that reason, it makes sense to delegate the cloud as the fourth border type, up for regular protection, just like the land, sea and air borders.

At the same time, some synergies already exist between border management and cybersecurity. Boin *et al.* discuss how the EU has built up its ability to respond to transboundary crises as a multi-entity, "trans- or cross-national coalition of public, private, and non-governmental actors" (2013, p.4). What was at first a set of disadvantages for the coalition of member states (it is often "hard to share information, organize a rapid response, and speak with one voice" at the EU level), begins to look like a head start in the emerging challenges in the face of globalization. Cross border cooperation is key for managing transborder crises like the pandemic or cyberthreats, and this is rarely a straightforward or easy task, even among kindred neighbours. This begins with the state border management and especially IBM. Border management by definition encompasses international relations because there is no such thing as a border if another state does not exist on the other side of it, whether those relations are strategic, tense or favourable. Border authorities already have vast experience in this domain, as well as networks and procedures in place for this kind of information exchange and cooperation, which is where the fledgling cybersecurity sector could benefit.

In terms of the innovation needed to meet evolving security needs, border management faced similar challenges as the cybersecurity domain, as the civic interest in securing borders dramatically outpaced the governmental ability to modernize them. By the time a security vulnerability is detected in either area, it is oftentimes because a criminal has already tried or succeeded in exploiting it. Border management in the EU has been able to reform many of its traditional methods in part due to the cleverness of the smugglers encountered during the migration crisis, which brought a high degree of attention to securing the borders. Equally, on a more positive note, globalization brought many opportunities for trade and commerce that also needed better systems of processing for speedier passage and secure handling.

There is also the classic struggle for any type of authority to remain two steps ahead of a potential wrongdoer in order to prevent misdeeds, from a teacher in a classroom to a border guard performing checks to a CERT building protections against hackers. The authority always has to remain wary of new and developing methods the criminal might try to use, with the disadvantage that they have to operate within the confines of the law and their mandate, whereas a criminal does not. In their assessment of challenges in combatting cybercrime, Hayes *et al*. talk about how it is not necessarily the technical ability stopping LEAs from keeping ahead of emerging criminal tactics, but that their legal mandate does not always permit them to use the means necessary in order to meet the challenge (2015, p.19). One can argue that this is a good thing, because those legal restrictions also keep LEAs from conducting 'unwarranted surveillance' (2015, p.35) on the general public. Regardless, it is another hurdle that both domains must face and can only be resolved with better investment in the right practices, commitment to human rights, and proper, legal channels for information flows.

4.4 Findings

This section shall summarize the findings of the research as a whole. In short, exploratory research demonstrated that the cloud border exists and is in need of protection as much as any traditional physical border. This proves difficult as, like a cloud, this border is extremely porous. Nonetheless, as an umbrella protects against precipitation, cyber border management can serve the goal of protection from cloud threats. Cross-border – not border*less* – cooperation is a key facet of cloud border protection. The EU has proven itself a trailblazer in the area of internet regulation with the GDPR, as well as the freedom of movement in the Schengen zone, but has become a greater target

for hybrid threats in recent years. However, the EU has committed to continue to strive for a middle-ground between the US-China dichotomy between free-for-all and censorship models, and once the balance is struck, other democracies will take notice. The Strategic Compass proves that commitment, but more actionable goals and private sector involvement are critical to ensure its success.

As a relatively new industry, cybersecurity is lacking the institutional memory and experience to adequately address coordination amongst governments and other state actors, and has not yet positioned itself as beneficial for private sector cooperation. Border management has dealt with centuries of similar challenges and is best-equipped to integrates the overlapping cybersecurity risks in regards to external threats to the state. The EU's concept of IBM is the roadmap for coordination and cooperation with intra-agency, inter-service and international partnerships, into which cloud border protection should be enveloped.

BM and cybersecurity also share similar political struggles, in that they present a moral dilemma between prioritizing regulation against rights and freedoms; privacy against security. There is no easy answer for these debates, but it is worth viewing them simultaneously in the context of state security, as they are so closely intertwined.

The border management industry is therefore dually equipped to address cybersecurity against external threats. First, external threats are a border issue by nature, as they enter the system by crossing the cyber boundary into the state. Secondly, BM is cross functional, adaptive and well-respected as an ancient function of the state, and is therefore capable of mentoring and integrating the new industry by sharing its institutional knowledge and outreach.

Finally, this study has examined the case study of Belarus, and found that the biggest failure of the crisis was the inability of the border management system to recognize the hybrid threats coming from the cloud before it became a physical border issue. The marriage of these two industries would address hybrid threats much more effectively.

Chapter 5 – Conclusion

This research study has explored my hypothesis that cybersecurity belongs in the border management domain, using the cloud as the label for the fourth border type after land, sea and air. Scholarly theories and discussions in cybersecurity and border management were examined. Hybrid threats see the biggest overlap between the two fields, but there are synergies discovered in theoretical application to threats facing both, as well as ethical considerations for the balance of security and citizens' rights to privacy. Integrated border management presents the best tool for confronting cybersecurity issues in the cloud.

The Belarussian case study of hybrid warfare on the EU's external borders exemplifies how the integration of cyber and border policy could create the cloud boundary, and could have helped mitigate or even prevent the crisis from occurring in the first place.

Similarities between the two fields were then more closely examined in order to position the argument that there is a shared history that could be beneficial in further guarding of the cloud. The private sector emerged as an integral player in two ways. On one hand, external experience is usually necessary and outsourced by governments in complex topics such as these. Secondly, they are the primary collectors of private data and their cooperation must be encouraged in order to have any chance at including them in holistic cybersecurity strategy as well as at allowing themselves to be regulated. However, for the regulation reason, the private sector tends to have little interest in cybersecurity, but high interest in border management in order to avoid trade barriers. By merging these topics into the cloud border, there may be less resistance to corporate buy-in.

Policy recommendations are laid out for a way forward. Hinging on the fact that the EU has already proven itself as a trailblazer in regulatory online policy through the GDPR, I propose the development of a new cloud-guard job profile at border crossing points, cloud CERTs, which could also present a model for other states to consider. I also recommend that further research into this area, using a range of methods, be carried out in order to have a more complete picture of the issues and possible solutions.

External borders are the points of entry for criminals to target the security of the state. It is up to states to recognize what is already happening, and set up a proper hybrid response by integrating national cybersecurity into its border institutions. This is only possible via the introduction of a fourth border type in addition to land, sea and air border protection: The Cloud.

Bibliography

"Regulation 2016/1624/EU on the European Border and Coast Guard" (2016) *Official Journal.* L251/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R1624 (Accessed: January 6, 2023).

€18 billion support package to Ukraine for 2023. (9 November 2022) *European Commission*. Brussels: Press Corner. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6699 (Accessed: January 5, 2023).

Andreas, P. (2003) "Redrawing the line: Borders and security in the twenty-first century," *International Security*, 28(2), pp. 78–111. Available at: https://doi.org/10.1162/016228803322761973.

Barrinha, A. and Christou, G. (2022) "Speaking sovereignty: The EU in the Cyber Domain," *European Security*, 31(3), pp. 356–376. Available at: https://doi.org/10.1080/09662839.2022.2102895.

Bellanova, R., Carrapico, H. and Duez, D. (2022) "Digital/sovereignty and European Security Integration: An introduction," *European Security*, 31(3), pp. 337–355. Available at: https://doi.org/10.1080/09662839.2022.2101887.

Blair, M. (2016) *An analysis of the migration policies of the European Union and their effectiveness in managing the current migration crisis.* MA IDS Thesis Projects. 33. Available at: http://commons.cu-portland.edu/gradproj/33 (Accessed: January 5, 2023).

Blumenau, J. and Lauderdale, B.E. (2018) "Never let a good crisis go to waste: Agenda setting and legislative voting in response to the EU crisis," *The Journal of Politics*, 80(2), pp. 462–478. Available at: https://doi.org/10.1086/694543.

Boeke, S. and Broeders, D. (2018) "The demilitarisation of cyber conflict," *Survival*, 60(6), pp. 73–90. Available at: https://doi.org/10.1080/00396338.2018.1542804.

Boin, A., Busuioc, M. and Groenleer, M. (2013) "Building European Union Capacity to manage transboundary crises: Network or lead-agency model?," *Regulation & Governance*, 8(4), pp. 418–436. Available at: https://doi.org/10.1111/rego.12035.

Border Management and Security Programme (2022) *ICMPD*. Available at: https://www.icmpd.org/our-work/capacity-building/border-management-and-security-programme (Accessed: December 7, 2022).

Brandão, A.P. and Camisão, I. (2021) "Playing the market card: The Commission's strategy to shape EU cybersecurity policy," *JCMS: Journal of Common Market Studies*, 60(5), pp. 1335–1355. Available at: https://doi.org/10.1111/jcms.13158.

Bruycker, P.D. (2016) *The European border and Coast Guard: A new model built on an old logic*, *European Papers*. European Papers (www.europeanpapers.eu). Available at: https://www.europeanpapers.eu/en/e-journal/european-border-and-coast-guard-new-model-built-old-logic (Accessed: January 5, 2023).

Burwell, F.G. and Propp, K. (2020) “The European Union and the Search for Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World?,” *Atlantic Council*. Available at: https://www.jstor.org/stable/resrep26697 (Accessed: January 6, 2023).

Calderaro, A. and Blumfelde, S. (2022) “Artificial Intelligence and EU security: The false promise of digital sovereignty,” *European Security*, 31(3), pp. 415–434. Available at: https://doi.org/10.1080/09662839.2022.2101885.

Carrapico, H. and Barrinha, A. (2017) “The EU as a coherent (cyber)security actor?,” *JCMS: Journal of Common Market Studies*, 55(6), pp. 1254–1272. Available at: https://doi.org/10.1111/jcms.12575.

Chayes, A. and Chayes, A.H. (1998) *The new sovereignty: Compliance with International Regulatory Agreements*. Cambridge: Harvard University Press.

Christou, G. (2016) *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Basingstoke: Palgrave Macmillan.

Chulov, M. and Tondo, L. (2021) “Tourist visas and flights from Syria – the route to Europe via Belarus,” *The Guardian*, 12 November. Available at: https://www.theguardian.com/global-development/2021/nov/12/its-risky-but-ill-go-anyway-migrants-desperate-to-reach-europe-via-belarus (Accessed: January 5, 2023).

Coon, C. (2021) “Is the Schengen area worth saving?,” *Claremont-UC Undergraduate Research Conference on the European Union*, 2021(01), pp. 11–21. Available at: https://doi.org/10.5642/urceu.202101.05.

Couture, S. and Toupin, S. (2019) “What does the notion of ‘sovereignty’ mean when referring to the digital?,” *New Media & Society*, 21(10), pp. 2305–2322. Available at: https://doi.org/10.1177/1461444819865984.

Crawford, K. (2016) *Artificial Intelligence's white guy problem*, *The New York Times*. The New York Times. Available at: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html (Accessed: January 5, 2023).

De Spiegeleire, S., Jans, K. and Rujan, A. (2017) *New Security Threats and Opportunities: The Other Side of the Security Coin*. Hague Centre for Strategic Studies. Available at: https://www.jstor.org/stable/resrep12598 (Accessed: January 5, 2023).

Dempsey, J.X. and Flint, L.M. (2003) “Commercial data and national security,” *The George Washington Law Review*, 72(6), pp. 1459–1502. Available at: https://doi.org/https://heinonline.org/HOL/LandingPage?handle=hein.journals/gwlr72&div=59&id=&page=.

Euronews (2021) “EU 'stands in Solidarity' with Latvia, Lithuania and Poland over Belarus,” 3 September. Available at: https://www.euronews.com/2021/09/03/eu-stands-in-solidarity-with-latvia-lithuania-and-poland-over-belarus (Accessed: January 7, 2023).

European border and Coast Guard: 10 000-strong standing corps by 2027: News: European parliament (17 April 2019) *News*. European Parliament. Available at: https://www.europarl.europa.eu/news/en/press-room/20190410IPR37530/european-border-and-coast-guard-10-000-strong-standing-corps-by-2027 (Accessed: January 5, 2023).

Fahey, E. (2014) "The EU's cybercrime and cyber-security rulemaking: Mapping the internal and external dimensions of EU Security," *European Journal of Risk Regulation*, 5(1), pp. 46–60. Available at: https://doi.org/10.1017/s1867299x00002944.

Fröhlich, C. and Müller-Funk, L. (2020) *Perceiving Migration Crises: A view from the European neighbourhood*. rep. EC Horizon 2020. Available at: https://www.magyc.uliege.be/about/wp4/ (Accessed: January 7, 2023).

General Secretariat of the Council (2022) *A Strategic Compass for Security and Defence*. Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (Accessed: January 6, 2023).

Gerstein, D.M., Atler, A., Davenport, A.C., Grill, B., Kadlec, A. and Young, W. (2018) *Managing international borders: balancing security with the licit flow of people and goods*. RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE290.html (Accessed: January 7, 2023).

Gillis, A.S. (2021) *What is a VPN? definition from searchnetworking, Networking*. TechTarget. Available at: https://www.techtarget.com/searchnetworking/definition/virtual-private-network (Accessed: January 5, 2023).

Gilpin, R.G. (1984) "The richness of the tradition of political realism," *International Organization*, 38(2), pp. 287–304. Available at: https://doi.org/10.1017/s0020818300026710.

Goel, S. (2020) "National Cyber Security Strategy and the emergence of strong digital borders," *Connections: The Quarterly Journal*, 19(1), pp. 73–86. Available at: https://doi.org/10.11610/connections.19.1.07.

Grainger, A. (2010) *The role of the private sector in border management reform.* Washington DC: The World Bank.

Häggström, H. (2021). "Hybrid threats and new challenges for multilateral intelligence cooperation," in *Hybrid warfare: Security and asymmetric conflict in international relations*. Bloomsbury Academic, pp.132-144.

Hayes, B., Jeandesboz, J., Simon, S., Mitsilegas, V. and Scherrer, A. (2015). *The law enforcement challenges of cybercrime: are we really playing catch-up?* EPRS: European Parliamentary Research Service.

Heldt, A. (2019) “Let's meet halfway: Sharing new responsibilities in a Digital age,” *Journal of Information Policy*, 9(1), pp. 336–369. Available at: https://doi.org/10.5325/jinfopoli.9.1.0336.

High Representative of the Union for Foreign Affairs and Security Policy (2020) *The EU’s Cybersecurity Strategy for the Digital Decade*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (Accessed: January 5, 2023).

Hoffman, F. (2014) “Hybrid warfare and challenges,” in *Strategic Studies*. 2nd edn. London: Routledge, pp. 329–337.

Hubert, D. (2021) *Digital Markets Act*. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662641 (Accessed: January 7, 2023).

Hybrid threats (no date) *Defence Industry and Space*. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en (Accessed: January 6, 2023).

Jain, A.K., Ross, A. and Pankanti, S. (2006) “Biometrics: A tool for information security,” *IEEE Transactions on Information Forensics and Security*, 1(2), pp. 125–143. Available at: https://doi.org/10.1109/tifs.2006.873653.

Joint Framework on countering hybrid threats: A European Union response (2016) European Commission, 6 April, 52016JC0018.

Jupillat, N. (2015) *Armed attacks in cyberspace: The unseen threat to peace and security that redefines the law of State responsibility*, University of Detroit Mercy Law Review 92(2) pp.115-130. Available at: https://ssrn.com/abstract=2772798

Kapucu, N. and Hu, Q. (2022) “An old puzzle and unprecedented challenges: Coordination in response to the COVID-19 pandemic in the US,” *Public Performance & Management Review*, 45(4), pp. 773–798. Available at: https://doi.org/10.1080/15309576.2022.2040039.

Keohane, R.O. (2002) “Ironies of sovereignty: The European Union and the United States,” *JCMS: Journal of Common Market Studies*, 40(4), pp. 743–765. Available at: https://doi.org/10.1111/1468-5965.00396.

Keukeleire, S. and MacNaughtan, J. (2008) *The foreign policy of the European Union*. New York: Palgrave Macmillan.

Kocs, S.A. (1995) “Territorial disputes and Interstate War, 1945-1987,” *The Journal of Politics*, 57(1), pp. 159–175. Available at: https://doi.org/10.2307/2960275.

Kumar, R. (2014) *Research methodology: A step-by-step guide for beginners*. Los Angeles: SAGE.

Lapsley, G.T. (1900) “A Study in English Border History.” *The American Historical Review* 5(3) pp.440–466. https://doi.org/10.2307/1835236.

Lété, B. (2021) *Implementing the EU cybersecurity strategy: Recommendations from the European Cyber Agora, The German Marshall Fund of the United States*. Available at: https://www.gmfus.org/news/implementing-eu-cybersecurity-strategy-recommendations-european-cyber-agora (Accessed: January 5, 2023).

Liboreiro, J. (2021) "Allegations, lawsuits and damning reports: How Frontex became the most contentious EU agency," *Euronews*, 26 August. Available at: https://www.euronews.com/my-europe/2021/07/29/allegations-lawsuits-and-damning-reports-how-frontex-became-the-most-contentious-eu-agency#:~:text=In%20a%20report%20released%20in,to%20fulfil%20its%20expanded%20mandate (Accessed: January 5, 2023).

Lindblom, S. and Castrén, J. (2021) "Implementation of European Union Security Strategies in the context of Integrated Border Management," *Remapping Security on Europe's Northern Borders*, pp. 85–99. Available at: https://doi.org/10.4324/9781003096412-7.

Lonardo, L. (2021) "EU Law Against Hybrid Threats: A First Assessment," *European Papers - A Journal on Law and Integration*, 6(2), pp. 1075–1096. Available at: https://doi.org/10.15166/2499-8249/514.

Mann, M., Warren, I. and Kennedy, S. (2018) "The legal geographies of transnational cyber-prosecutions: Extradition, human rights and forum shifting," *Global Crime*, 19(2), pp. 107–124. Available at: https://doi.org/10.1080/17440572.2018.1448272.

Mchangama, J. (2022) "The real threat to social media is Europe," *Foreign Policy*, 25 April. Available at: https://foreignpolicy.com/2022/04/25/the-real-threat-to-social-media-is-europe/ (Accessed: January 5, 2023).

Meyers, E. (2000) "Theories of international immigration policy-A comparative analysis," *International Migration Review*, 34(4), p. 1245. Available at: https://doi.org/10.2307/2675981.

Moore, J. B. (1899) "The Alaskan Boundary." *The North American Review*, 169(515) pp.501–15. *JSTOR*, http://www.jstor.org/stable/25104886. Accessed 7 Feb. 2023.

Nichols, G.E.W. (2022) *"Playing Chicken" with Populations Migrant Instrumentalization and the Schengen Area*. Master's thesis. Available at: https://hdl.handle.net/11250/3010471 (Accessed: January 6, 2023).

Ntoutsi, E. *et al.* (2020) "Bias in data-driven Artificial Intelligence Systems—an introductory survey," *WIREs Data Mining and Knowledge Discovery*, 10(3). Available at: https://doi.org/https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1356.

Oliveira Martins, B., Lidén, K. and Jumbert, M.G. (2022) "Border Security and the digitalisation of sovereignty: Insights from EU Borderwork," *European Security*, 31(3), pp. 475–494. Available at: https://doi.org/10.1080/09662839.2022.2101884.

Pelley, S. (2021) *Whistleblower: Facebook is misleading the public on progress against hate speech, violence, misinformation, CBS News*. CBS Interactive. Available at:

https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-misinformation-public-60-minutes-2021-10-03/ (Accessed: January 7, 2023).

Pluim, M. and Hoffman, M. (2015) *Integrated Border Management and Development*. ICMPD working paper 08. Available at: https://www.pragueprocess.eu/en/migration-observatory/publications/33-reports/171-integrated-border-management-and-development-icmpd-working-paper-08 (Accessed: January 7, 2023).

Polner, M. (2011) "Coordinated border management: from theory to practice," *World Customs Journal*, 5(3), pp. 49–64. Available at: https://doi.org/https://www.researchgate.net/publication/309556915_Coordinated_border_management_From_theory_to_practice.

Provan, K.G. and Kenis, P. (2007) "Modes of network governance: Structure, management, and effectiveness," *Journal of Public Administration Research and Theory*, 18(2), pp. 229–252. Available at: https://doi.org/10.1093/jopart/mum015.

Puddephatt, A. (2020) "Governing the Internet: The Makings of an EU Model," *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*, edited by Hobbs, C., European Council on Foreign Relations, pp.13-26.

Ramji-Nogales, J. (2022) "Ukrainians in Flight: Politics, race, and Regional Solutions," *AJIL Unbound*, 116, pp. 150–154. Available at: https://doi.org/10.1017/aju.2022.22.

Ratner, S.R. (1996) "Drawing a better line: *uti possidetis* and the borders of New States," *American Journal of International Law*, 90(4), pp. 590–624. Available at: https://doi.org/10.2307/2203988.

Read, T. (1963) "Nuclear tactics for defending a border," *World Politics*, 15(3), pp. 390–402. Available at: https://doi.org/10.2307/2009469.

Refugee crisis in Europe: Aid, statistics and news: USA FOR UNHCR (2021) *Refugee Crisis in Europe: Aid, Statistics and News*. Available at: https://www.unrefugees.org/emergencies/refugee-crisis-in-europe/ (Accessed: January 7, 2023).

Roloff, R. (2020) "COVID-19 and No One's World," *Connections*, 19(2), pp. 25–37. Available at: https://doi.org/https://www.jstor.org/stable/26937607.

Sadik, G. and Ceren, K.A.Y.A. (2020) "The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management," *Uluslararası İlişkiler Dergisi*, 17(68), pp. 145–160. Available at: https://doi.org/https://www.jstor.org/stable/26980741.

Sargana, T.H., Sargana, M.H. and Anns, M. (2020) "Approaches to international information security and the discourse of Cyberspace," *Masyarakat, Kebudayaan dan Politik*, 33(4), p. 331. Available at: https://doi.org/10.20473/mkp.v33i42020.331-338.

Sassen, S. (1996). Losing Control? Sovereignty in an Age of Globalization. New York: Columbia University Press.

Satariano, A. (2021) *Facebook hearing strengthens calls for regulation in Europe.* The New York Times. Available at: https://www.nytimes.com/2021/10/06/technology/facebook-european-union-regulation.html (Accessed: January 5, 2023).

Schengen area - the 27 member countries of the Schengen Zone (2023) *SchengenVisaInfo.com*. Available at: https://www.schengenvisainfo.com/schengen-visa-countries-list/ (Accessed: January 5, 2023).

Schimmelfennig, F. (2018) "European Integration (theory) in times of crisis. A comparison of the euro and Schengen crises," *Journal of European Public Policy*, 25(7), pp. 969–989. Available at: https://doi.org/10.1080/13501763.2017.1421252.

Siripurapu, A. and Merrow, W. (2021) *Social Media and Online Speech: How Should Countries Regulate Tech Giants?* Council on Foreign Relations. Available at: https://www.cfr.org/in-brief/social-media-and-online-speech-how-should-countries-regulate-tech-giants (Accessed: January 7, 2023).

Speier, M. (2021) *Covid-19 and the threat to press freedom in central and Eastern Europe, Council on Foreign Relations*. Council on Foreign Relations. Available at: https://www.cfr.org/in-brief/covid-19-and-threat-press-freedom-central-and-eastern-europe (Accessed: January 7, 2023).

Strengthening Border Security Through Enhanced Frontline Collaboration (2017) *INTERPOL*. Available at: https://www.interpol.int/en/News-and-Events/News/2017/Strengthening-border-security-through-enhanced-frontline-collaboration (Accessed: January 5, 2023).

Tardy, T. (2022) *War in Europe: preliminary lessons*. NDC Public Affairs Office. Available at: https://www.ndc.nato.int/news/news.php?icode=1696 (Accessed: January 7, 2023).

Terpan, F. and Saurugger, S. (2020) "Soft and hard law in times of crisis: Budget Monitoring, migration and cybersecurity," *West European Politics*, 44(1), pp. 21–48. Available at: https://doi.org/10.1080/01402382.2020.1738096.

Thumfart, J. (2021) "The Covid-crisis as catalyst for the norm development of digital sovereignty. Building barriers or improving digital policies?," *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.3793530.

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K. and McCue, M. (2018) *Addressing Hybrid Threats*. rep. CATS in cooperation with Hybrid CoE. Available at: https://www.hybridcoe.fi/publications/addressing-hybrid-threats/ (Accessed: January 7, 2023).

Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A.K. (2004) "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, 92(6), pp. 948–960. Available at: https://doi.org/10.1109/jproc.2004.827372.

Veit, R.-D. (2022) “Safeguarding regional data protection rights on the global internet—the European approach under the GDPR,” *Personality and Data Protection Rights on the Internet*, pp. 445–484. Available at: https://doi.org/10.1007/978-3-030-90331-2_18.

Von der Leyen, U. 2021. *Statement by the President: Situation in Belarus*. November 28, Vilnius.

Walters, W. (2002) “Mapping Schengenland: Denaturalizing the border,” *Environment and Planning D: Society and Space*, 20(5), pp. 561–580. Available at: https://doi.org/10.1068/d274t.

Waltz, K.N. (1990) “Realist thought and Neorealist theory,” *Journal of International Affairs*, 44(1), pp. 21–37. Available at: https://doi.org/https://www.jstor.org/stable/24357222.

Weimann, G. (2004) *Www.terror.net: How modern terrorism uses the internet*. Washington, DC: United States Institute of Peace.

Weiss, M. and Jankauskas, V. (2018) “Securing cyberspace: How states design governance arrangements,” *Governance*, 32(2), pp. 259–275. Available at: https://doi.org/10.1111/gove.12368.

Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P., 2021. *Hybrid warfare: Security and asymmetric conflict in international relations*. I.B. TAURIS: Bloomsbury Academic.

Wesselink, C. (2022) *Stateless, rightless and weaponized. The European Union's human rights contradictions in the EU-belarus border crisis. Wesselink, 6151701, Utrecht University Student Theses Repository Home*. Available at: https://studenttheses.uu.nl/handle/20.500.12932/42917 (Accessed: January 5, 2023).

Witney, N. (2022) *The EU's strategic compass: Brand New, already obsolete, ECFR*. Available at: https://ecfr.eu/article/the-eus-strategic-compass-brand-new-already-obsolete/ (Accessed: January 5, 2023).

Wolford, B. (2022) *What is GDPR, the EU's new Data Protection Law? GDPR.eu*. Available at: https://gdpr.eu/what-is-gdpr/ (Accessed: January 5, 2023).

Wu, T.S., (1996). “Cyberspace sovereignty-the Internet and the international system,” *Harvard Journal of Law & Technology, 10.* pp.647-666). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/2227

Zhu, R. (1970) *Pattern, practice, and potency of Information Systems Security Research: A methodological perspective*, *Semantic Scholar*. Available at: https://www.semanticscholar.org/paper/Pattern%2C-Practice%2C-and-Potency-of-Information-A-Zhu/dd7fe39da40ce5e955316dc8ae912d479747a42e (Accessed: January 5, 2023).