Hatfield Graduate Journal of Public Affairs

Volume 5
Issue 1 *The Hatfield Graduate Journal of Public Affairs*

Article 10

May 2021

The European Union: Data Protection for Economic Competition and Regional Security

Matthew D. Wurst
Portland State University

Recommended Citation
Wurst, Matthew D. (2021) "The European Union: Data Protection for Economic Competition and Regional Security," *Hatfield Graduate Journal of Public Affairs*: Vol. 5: Iss. 1, Article 10.
https://doi.org/10.15760/hgjpa.2021.5.1.10

The European Union:
Data Protection for Economic Competition and Regional Security

The collection and use of personal data is being increasingly scrutinized by governments and the European Union (EU) has been attempting to handle the development of data protection based progressive protections to protect its citizens data and right to privacy. With the reemergence of Russia in challenging the state of affairs within Europe, their illegal seizure of the Crimea from Ukraine demonstrated the lengths Russia will go to in order to preserve its sphere of influence. Furthermore, Russia's use of cyber tactics and hybrid warfare has caused many in Europe to become more concerned for their security. When viewed through the lens of Power Transition Theory, the actions of the EU have indicated that it has been working to ensure it is protected from a dissatisfied actor's potential rise. Indeed, with Russia's investment into using cyber-attacks, the EU has acted to protect itself, its members, and its citizens.

Matthew D. Wurst
Portland State University

INTRODUCTION

The European Union (EU) is a configuration of 27 member states on the European continent that have primarily integrated their traditionally sovereign economies to compete within the global economy. The EU's jurisdiction has expanded beyond traditional economic policy to encompass several other policy domains that tangentially relate to economic regulation. Following the collapse of the Soviet Union, the states of Europe were able to focus on restructuring themselves into the modern EU to match the new security dynamics in Europe. Indeed, the EU was finally able to achieve its long-term goal of creating a single European market, which significantly shifted power dynamics in centralizing its influence and expanding membership within Europe.

10.15760/hgjpa.2021.5.1.10

When framed through the lens of Power Transition Theory, the actions of the EU demonstrate its need to ensure security for itself, its member states, and its citizens. As the world has become increasingly globalized, a reliance on data has played a large role in the growing prevalence of the Internet and technology in the international economy. Because of the sheer amount of data available, bad actors and dissatisfied states can collect large amounts of data with the intent to possibly influence the internal dynamics of other states. Thus, the EU has proactively enacted a progressive data protection regime, starting in the 1990s, and has remained vigilant in ensuring its citizens' progressive privacy and data protection rights at the international level.

As Russia has aggressively reasserted its regional power within Europe, concerns over new areas of conflict have emerged. Indeed, since the end of World War II, the European continent has enjoyed relative stability and has been free from violent conflict. However, with the development of technology and the Internet, states are now able to infringe on another's sovereignty with relative ease. This emergence of hybrid warfare and the deployment of cyber-attacks has raised new concerns of how to maintain the security of the EU and its members from these kinds of attacks.

Though data privacy has not yet been recognized as an internationally protected human right enforceable by international law globally, the EU has created its own regime of international law as the foundation for its progressive laws within Europe. Due to this, the EU has been able to enact privacy and data protection laws through the lens of economic regulation, but also to ensure the security of the EU and its members from the increased introduction and reliance of technology in conflict between states.

POWER TRANSITION THEORY

Introduced in 1958, Power Transition Theory (PTT) was developed to account for the incidence of wars fought for control of the international system among the very strongest of states (Lemke 2002, 21).[1] PTT does establish a hierarchical system of international relations as an independent theory of international relations and power dynamics. Specifically, PTT focuses on the "maintenance of and changes to the

[1] Power Transition Theory was first introduced by A.F.K Orgnaski in *World Politics* (1958) to describe a hierarchical international structure that explains the actions between states, specifically in contrast to Balance of Power theory within realism, in particular a dominant and a challenging state.

international system," where the satisfaction of each state plays a significant role in its actions and outlook on the international system (Lemke 1997, 24).

However, the prevalence of realism and liberalism in explaining the international community has led to PTT exhibiting aspects of both theories (Lemke 1997, 24). In his influential book *Regions of War and Peace*, Lemke expands Orgnaski's theory beyond its original application to the great or major powers applying the theory to regional hierarchies of states (2002). In the realist vein, PTT describes how the internal growth of a state impacts its relative power which is constantly changing. The "combination of power parity between challenger and dominant state combined with the challenger's negative evaluation of the status quo provides the necessary condition for war," specifically great power war, and therefore control of the international system (Lemke 1997, 24). In the liberal vein, PTT allows for the dominant state to establish its own hierarchy within the international community. The most prominent example is after World War II when the United States broke with traditional balance of power realism governing international relations to establish a liberal international order. Lemke extends this theory to include regions within the international community, allowing for the examination of regional international relations and the emergence of regional hegemons (1997, 25). Although a regional hegemon has accumulated more power than its regional neighbors, it remains significantly less powerful than the global hegemon.

As with any theory, there are a few issues with PTT and how it is applied in the real world. Chief among these issues is the ability of the theory to choose which states that are rising in its power are challengers and which are not, as well as identifying revisionist goals in a possible challenger to the hegemonic control of the international system (Lemke 1997). For example, there has been a significant amount of academic research and public resources dedicated to understanding the relationship between Russia and the United States, yet significantly less research has been conducted on the German-American relationship. Both Russia and Germany have seen significant economic and regional growth since the end of the Cold War and are considered important players at the international level. Research on the relationship between member states and the policies that are accepted by the EU shows there is a general consensus that Germany is the unofficial 'leader' following the Great Recession in 2008 (Fix 2018).[2] Germany, however, is an important ally of the United States and is therefore not considered a threat to

[2] While Fix ultimately focuses on the role that Germany plays in the EU's response to the crisis in Ukraine following the Russian invasion and occupation, the role of Germany within the EU is displayed and is significant enough to span more than just the response to the Ukrainian Crisis.

American hegemony. Russia, on the other hand, is an active instigator of conflict that has been involved in re-establishing its role as a regional power in Europe by engaging in conflict with Georgia and Ukraine. Furthermore, it is an indisputable fact by the American intelligence community of Russian involvement in the 2016 General Election, further demonstrating Russia's active role in undermining the status quo (S. Rpt. 116-290).

THE RIGHT TO PRIVACY AND DATA PROTECTION

To this day, the Universal Declaration of Human Rights (UDHR) by the United Nations General Assembly (UNGA) remains the defining document on human rights that is widely accepted by the majority of states in the international community. Unlike many of the other rights established in the UDHR, the right to privacy is still not completely defined within the domestic sphere of many states. Despite this inconvenience, the right to privacy is an established right under international human rights law, and of particular importance is connecting data protection to the right to privacy.

Article 12 of the UDHR outlines the international human right to privacy,[3] however there is another significant piece of international law that covers the right to privacy: The International Covenant on Civil and Political Rights (ICCPR). In Article 17, the right to privacy is laid out in two sections. The first establishes the right to privacy and the second provides an enforcement mechanism for states to enact legal protections for the right to privacy.[4] Upon examining the *travaux préparatoires,* the official record of negotiation between signatories of a treaty, behind both the UDHR and ICCPR, the right to privacy was included in discussions as the treaties developed, not necessarily as an original right in the first draft (Diggleman and Cleis 2014, 457). Further scrutiny reveals that the right to privacy is meant to guarantee against infringement to individuals by the state or persons, whether they be natural or legal (United Nations 1994). Krishnamurthy (2020) emphasizes that the right to privacy includes ensuring that "information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it" (27). The implications are impactful by

[3] Article 12 reads: **"**No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[4] Article 17 specifically reads:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

serving as a basis for the EU to pursue the protection of privacy and data protection. The EU has continued its push for data protection as a human right as technology becomes more integrated into everyday life. This is foundational to the EU and is enshrined within the European Convention of Human Rights' (ECHR) language concerning the right to privacy in Article 8.[5]

Data is important in determining and protecting the right to privacy and can be generated about people without their knowledge or consent, whereby the most meaningless or complex information can be saved and processed electronically (Boehme-Nebler 2016). The abundance of data available for states to record and process has dawned the concept of data protection. Governments have derived their concern for their citizens and their own data after seeing the costs of big data collection. It is inconceivable to comprehend the sheer amount of "data being collected, in so many ways, that it is practically impossible to give people a meaningful way to keep track of all the information about them that exists out there, much less to consent to its collection in the first place" (Mundie 2014). The remaining problem is that even when citizens consent to a user agreement, they may not understand how, when, or where their data is used by an entity.

Therefore, the objective of data protection is to secure the individual's human dignity and personal development because, without some form of inviolable privacy, an individual's personality cannot develop successfully (Boehme-Nebler 2016, 223). It is this link to the individual's inherent need for privacy that connects data protection with human rights and, by extension, international law. In particular, the EU's continued economic integration has meant that data and data protection have become cemented in the EU's jurisdiction and at least regionally within Europe, international law. Data protection within the EU refers to efforts aimed at protecting Europeans' fundamental right to privacy from infringement or interference by either private or public actors.

[5] The ECHR was adopted on 4 November 1950 and came into force in 1953. Article 8 specifically states:

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

POWER TRANSITION THEORY AND THE EUROPEAN UNION'S PUSH FOR DATA PROTECTION

There is a reason beyond simple regulation for the EU's aggressive stance on data protection: data protection is essential for the security of the EU and its members. By including data protection within its jurisdiction, the EU's regulations serve a dual purpose of economic regulation and security. Following PTT, this is due to the EU's wariness of the emergence of and rejection by Russia to current regional power dynamics.

The EU represents the member states' need to remain economically relevant internationally. Important in understanding regional power dynamics, economic competition is directly relevant to the amount of power and influence the EU accumulates within the region. The European Commission has stated previously that the EU's goal is "to become the most competitive and dynamic knowledge-based economy in the world," indicating economic ambitions for international competition (Kugler, Fisunoglu, and Yesilada 2015). Indeed, the EU is now often considered a singular actor pursuing its interests within international relations, to which PTT provides interesting insight behind European relations.

PTT approaches international relations recognizing both horizontal and vertical forms of integration within the international and regional communities. Thus, the EU remains an important entity for both Europe and the international system. PTT demonstrates that within a hierarchical structure, the most powerful nations or entities attempt to manage the regional dynamics, meaning that disagreeing nations who are dissatisfied will emerge to challenge the prevailing structures (Kugler et. al. 2015, 49). This is the precise relationship occurring with the EU and Russia within Europe, exacerbated by the emergence of hybrid warfare and cyber tactics that rely on access to data. Member states, by banding together through integration, ensure that the EU is a singular entity that represents the security of the majority of European nations, particularly for international economic competition.

Concerning data protection, the EU has recognized that "promoting high standards of data protection and facilitating international trade" and security are essential (European Commission 2017). Data represents both a tremendous trade commodity and social asset, where a natural tension between economic welfare and the protection of fundamental rights presents a conflict for the EU in its role as a regulator (Yakovleva 2018, 478). By constituting data protection as an economic regulation, the EU can properly regulate the use and collection of data, and simultaneously protect the fundamental rights of its citizens and the security of its members. Difficulty remains in grounding data protection in international law

because "[n]either public international law nor international trade law provide for adequate mechanisms to balance trade liberalization objectives against non-economic human rights concerns" (Yakovleva 2018, 479). This means that the EU's approach to fundamental rights, such as privacy and data protection, is anchored in the ECHR and broader international human rights law. The regulations on data serve a dual purpose of economic regulation and security of member states through promotion of aggressive data protection law.

Given the complexity in establishing stringent standards for the economic regulation and protection of its member states, the progression of treaties that established the EU have increasingly given it the authority to protect the economic interests of its members and citizens of Europe in general. While not given the direct authority to engage in more traditional activities of foreign affairs that are reserved to states, the EU has established and understands its role in the current international problems through its Common Security and Defence Policy (CSDP) (EEAS 2016).

As PTT attempts to predict the power relations within Europe as a region, it remains important to understand the institutional restrictions placed on the EU by the member states. For example, the North Atlantic Treaty Organization (NATO) handles its European members' security policy and involvement, while the EU serves as the member states' coalition pooling their economic resources, with both organizations strengthening their members' individual power on the international stage. Indeed, because of this dual representation of member states, EU-NATO relations form a complex web of conflicting and coinciding jurisdictions and outcomes (Græger 2016). However, the EU's commitment of exclusive membership to solely European members demonstrates the largest consolidation of European resources and interests, while the influence of the United States and other members in NATO marks it more as a Western alliance rather than a solely European alliance. By extension, it is logical to apply PTT to the EU as it represents the most centralized significant voice of European interests. This implies that the EU has replaced a typical state as regional hegemon, and Russia is acting in accordance to its status as a rising and dissenting power to the EU's centrality to regional power dynamics.

DATA PRIVACY DIRECTIVE (1995) AND THE GENERAL DATA PROTECTION REGULATION (2016)

While PTT's importance is in attempting to predict regional power conflicts, which mostly results in violence between the hegemon and challenger, the EU has

achieved staving off Russia's increased influence within Europe by passing aggressive regulations concerning data protection. Indeed, while dynamics following the Cold War did not immediately indicate future friction between the EU and Russia, the EU has worked to peacefully secure its resources and interests from outside interference. In accordance with this goal, two significant pieces of legislation have been passed by the EU that attempt to create and enforce data protection standards by regulating its economic activity.

Starting in 1995, the EU passed what is known as the Data Privacy Directive (DPD). Enacted after years of discussion among the member states, its purpose was to accomplish the harmonization between members, to allow the free flow of information within the EU, and to provide a "high level of protection" concerning individual data privacy rights (Newman 2008, 74). With the dissolution of the Soviet Union, the EU became the central economic power player in Europe. Russia remained a power player in European affairs after its democratic transition and was generally welcomed by retaining its permanent status on the Security Council at the UN, acceptance into the G8 in 1997, and mostly retained credibility on the international stage.

The EU has continued to act in a fashion that guarantees the right to privacy and data protection. Guaranteed in the Treaty of Lisbon (2007), the EU holds the position that "the privacy of communications and the protections of personal data to be fundamental human rights" (Weiss and Archick 2016, 2). Protections cover the possession of all personal data gathered automatically or manually, allow individuals significant access to their data, and grant the ability for individuals to seek damages if necessary (Weiss and Archick, 2-3). Of particular interest is the DPD's requirement that mandates transfers of personal data out of the member state or EU only if the European Commission certifies that the country provides *adequate* levels of protections to that of the DPD.

The need for the European Commission to certify that another state has adequate protections means that states interested in trading directly with the EU also need similar protections in place. The EU's progressive measures towards data protection are rooted in both international economic law and international human rights law, which forces states that choose to trade with the EU to adhere to its rigorous standards. It is important not to underestimate the influence that security plays in these standards both for member states and its citizens. With the European Commission regulating who meets adequate protections, the EU is able to passively ensure the security of its member states by protecting the vast amount of data moving through economic activity against cyberattacks.

As Russia's significance has grown, the EU itself has significantly increased its stature in international relations as its own entity that represents its own interests separate from the member states. By the mid-2010s it was abundantly clear that new standards were needed to further advance the EU's jurisdiction and protection of its citizens privacy from interference to meet the advancing capabilities in technology. To this end, the EU was in the process of passing a new data protection law called the *General Data Protection Regulation* (GDPR), which was passed in April 2016 and became applicable to the member states in May 2018 when it officially repealed and replaced the DPD (Voss 2016).

The GDPR is aimed at establishing strict standards as a protection for its citizens and member states from increased Russian aggression in the region. Specifically, the GDPR states that adequacy decisions by the European Commission must certify that a third country has similar access to justice, rule of law, respect for human rights and fundamental freedoms, and a domestic infrastructure capable of ensuring the protection of personal data and privacy (IT GOVERNANCE 2019, 257-58). These conditions for certification of adequacy enforce the two main requirements under the GDPR's necessities for transferring data outside of the EU: the destination has been subject to an adequacy decision and that the transfer is subject to appropriate safeguards (IT GOVERNANCE 2019, 256).

The key protections offered by the GDPR are such that the private entities, as well as state actors, must comply with the high level of protection the EU has declared appropriate. Article 46 clearly states that there must be some form of legally binding and enforceable instrument between public and private authorities, binding corporate rules with standard data protection clauses, and complying with other protections aimed at protecting access to personal data and how data can be used. The European Commission has reflected that two years after implementation the "GDPR has successfully met its objectives of strengthening the protection of the individual's right to personal data protection…within the EU" (European Commission 2020, 4). The Commission also states that the influence of the GDPR is vast, demonstrating Europe's role as a global leader for the regulation of the digital economy, as well as protecting its citizens from data manipulation.

THE EMERGENCE OF HYBRID WARFARE, USE OF CYBER-ATTACKS AND RUSSIA'S DISSATISFACTION

There has been an increasing trend by states to develop and deploy resources utilizing the growth and prevalence of technology which has considerably focused

on data. Perhaps the most prominent proponent of these new tactics is Russia under the leadership of Vladimir Putin, particularly its 2014 aggression in Ukraine. Indeed, the aggressive acts by Russia, or by its proxies, should be considered acts challenging the EU's influence among states that Russia considers to be its traditional sphere of influence.

Technological advancements have allowed for states to develop tactics that cost less resources, human life, and can do more damage to their adversaries. Because of the evolving development and rapid deployment of new technology, the role that hybrid war plays has not been adequately defined in international law. Due to the lack of an exact definition of what constitutes hybrid warfare, the ability of the international community to identify and respond is a major factor in the increase and prevalence of hybrid warfare and deployment of cyberattacks. Indeed, according to Bachmann, the use of hybrid warfare was only first recognized in 2006 in the struggle between Hezbollah and the Israeli Defense Forces in the Second Lebanon War (2015, 78).

This begs the question of *what is* hybrid warfare. In 2010, NATO surmised a hybrid threat as "those [threats] posed by adversaries, with the ability to simultaneously employ conventional and nonconventional means adaptively in pursuit of their objectives" (NATO 2010). Furthermore, citing a 2011 NATO report, Aaronson et. al. stated that "[a]dmittedly, [a] hybrid threat is an umbrella term, encompassing a wide variety of existing adverse circumstances and actions" (2011, 115). Importantly, "[h]ybrid war is never announced officially and, so far, has never ended in a conventional war so far. It involves a permanent state of war-like situation with a variable intensity," and often involves covert and deniable activity (Simons, Danyk, and Maliarchuk 2020, 340). Without a concrete definition, hybrid warfare has emerged as a common tactic that states now have to regularly face or deploy their own form of. Importantly, hybrid warfare includes, but is certainly not limited to a variety of nonconventional tactics, yet it is the growing possibility of cyber-attacks that exhibit how the "use of new technologies" fall "within the scope of hybrid threats" (Bachmann 2015, 82).

This delineation is imperative. The use of cyber tactics refers "to a sustained computer-based cyber-attack by a state against the IT infrastructure of a target state" (Bachmann 2015, 82). This is not a limited behavior of states, however, as non-state actors may serve as both perpetrators and victims of a cyber-attack. To be effective, actors engaging in cyber tactics rely heavily on access to data and determine how they can use data to achieve their goals. There are multiple ways that data can be obtained, with the two most important for this analysis are data collected through illicit state actions via cyber-attacks and through everyday

economic activity. Indeed, data manipulation can occur through economic means whereby a company sells or analyzes data to influence consumer's choice or through states micro-targeting voters through the unlawful possession, analysis, and use of data in interfering with the democratic process (European Commission 2020, 3-4).

To states, cyber-attacks present a unique opportunity. Cyber tactics are potentially devastating and extremely difficult to defend against without infrastructure dedicated to such a task. Cyber tactics are additionally relatively "low-risk and low-cost means of achieving foreign and security policy aims and goals" (Simons et. al. 2020, 337). Indeed, "a solid and agreed upon legal framework to regulate [cyber tactics] does not yet exist," and remain cost effective and deniable to states (Simons et. al. 2020, 341). Currently, because of the lack of clarity in defining hybrid warfare and the use of cyber tactics, these terms have been used increasingly without presenting the differences. To be clear, hybrid warfare represents the totality of nonconventional tactics being deployed by states, while cyberattacks or cyber tactics is a *specific method of hybrid warfare*.

From the Russian perspective, expansion of both NATO and the EU into Eastern Europe and other areas of former Soviet dominance has occurred rather aggressively. Russian President Vladimir Putin stated in a 2007 speech concerning NATO specifically that, "I think it is obvious that NATO expansion does not have any relation with the modernization of the Alliance itself or with ensuring security in Europe. On the contrary, it represents a serious provocation that reduces the level of mutual trust. And we have the right to ask: against whom is this expansion intended?" (Putin 2007). Clearly Russia is dissatisfied with its current role within the international community, and specifically within the European sphere, and should be considered a dissatisfied state under PTT within the region. While the majority of states in Europe have joined both NATO and the EU, both organization's primary struggle is the handling of Russia's prominent aggression in reasserting itself. Accordingly, as Walt indicates, "Russia is still significantly weaker [than the Soviet Union]…but no longer a basket case" in international relations (2019, 33).

Of particular importance to this reemergence is why, where, and how Russia reacted. Both NATO and the EU represent the encroachment of the West into Russia's traditional domain. Moscow clearly believes that NATO represents the growth of the Western security apparatus, while the EU's growth following the Cold War represents equal encroachment in economic affairs. Russia feels its security is threatened by this expansion and took aggressive steps in 2008 to prevent Georgia from moving closer to NATO and the EU. Yet it was Russia's blatant

interference in Ukraine following its annexation of Crimea in 2014 that truly demonstrated Russia's dissatisfaction within Europe. Russia's dissatisfaction has manifested through its use of nontraditional tactics, like cyber-attacks, as demonstrated in both Georgia and Ukraine because of their efforts in courting Western influence.

While the conflict in Georgia represents much more traditional conflict, by 2014 Russia was deploying cyber tactics aimed at benefiting its goals of keeping Ukraine out of the EU's influence. Russia engaged in hybrid warfare by using cyber tactics, such as hacks targeted at Ukraine's telecommunications network and national security apparatus, to avoid the entanglements and consequences associated with traditional warfare and a possible military engagement with the United States (Limnell 2015, 527-28). As the world grappled with how to handle this resurgence of Russian aggression, the EU witnessed the cyber tactics Russia deployed in Ukraine that spelled immediate and long-term security needs for the EU. Indeed, cyber-attacks are not necessarily aimed at military targets, but towards public infrastructure, as demonstrated in the hack in December 2016 where Russian hackers were successfully able to shut down the power grid in North Kyiv for about an hour but remained unsuccessful in causing physical harm to the computing system (Simons et. al. 2020, 338-39).

Importantly, the tactics undoubtedly deployed by Russia in both Georgia and Ukraine often lack a direct link between the Russian government and the entities that orchestrate cyber tactics. As Hollis demonstrates, there is a lack of "substantive connection between the orchestrators of the cyberattacks and the Russian government" (2011). Giles indicates that while "there is no evidence of dedicated 'information troops' in the Russian military who could directly engage in local and regional areas," Russia learned from their successes and failures in Georgia (2016). Further building off its success in the Crimea, Russia demonstrated its abilities in a wide scale effort to influence the 2016 Presidential Election in the United States with a seemingly dedicated military force for this specific purpose, the Internet Research Agency (IRA) and the Main Intelligence Directorate of the General Staff of the Russian Army (GRU) (Mueller 2016). While the use of hybrid warfare and deployment of cyber tactics remains new to the arsenal of states, the Russian success in infiltrating American democracy "ranks among the greatest intelligence failures of modern times" and serves as a warning to the EU of Russia's capabilities (Sanger et. al. 2020).

THE POTENTIAL FOR POLITICAL INTERFERENCE FOR THE EU

Russia's aggressive stances towards Georgia and Ukraine justify the EU's concerns within Europe. Russia "eventually fought a short war with Georgia and Ukraine, seized Crimea from Ukraine, and used cyberattacks and 'hybrid warfare' to stop NATO [and the EU] from moving farther east and to *undermine the liberal order in Europe* (emphasis added)" (Walt 2019, 73). This goal suggests that Russia's dissatisfaction is ultimately aimed at challenging the EU for dominance within the European sphere of influence. Other than those directly impacted by Russian cyber interference, such as Ukraine and the United States, the EU remains vigilant against the advancement of Russia's capabilities and potential for interference to the EU. Importantly, the EU itself does not possess the capabilities to defend itself in terms of traditional security as European states have concentrated this power in NATO. Yet, this does not dispel the need for the EU to defend itself using the powers it has been granted within its jurisdiction to secure its members' interests, to which it has sought to regulate the use and dispersal of data from the EU with the DPD and GDPR.

Not only are states making efforts to protect their individual technological infrastructures and the data associated with the actions and operations of the state, but cyber tactics are increasingly deployed to obtain economic data from citizens of other states. Economic data protection is just as important to state sovereignty which demonstrates one of the central reasons for having the EU to begin with. The measures taken by the EU to protect the economic data of its citizens and member states is simultaneously providing security for its members and citizens.

An important example that highlights the need for these protections, and the severity of the consequences if action is not taken, is the massive breach into Equifax in 2017 that released a vast amount of personal data. Specifically, as a result, hackers were able to steal "the financial and personal information of approximately 147 million [people]," providing China with "detailed, organized information on nearly half the American population" (Rosenbach and Mansted 2019). This demonstrates the importance of data protection and the central role the right to privacy will continue to play as technology continues to develop and the use of cyber tactics and hybrid warfare become more prevalent.

Indeed, the steps taken by Russia under the leadership of President Putin have been directly aimed at curbing the influence and reach of the EU. While it was the invitation to Georgia and Ukraine to develop action plans for NATO membership that spurred Russia's involvement in Georgia in 2008, the subtle leanings of the Ukrainian people towards the pull of the EU was a significant factor in the 2014 seizure and subsequent annexation of Crimea in 2014 (Katerynchuck 2019 and Limnell 2015). The EU has also seen new levels of Euroscepticism, which refers to the efforts within EU member states that oppose further integrations, most

prominently with the departure of the United Kingdom from the EU. After seeing how disinformation greatly impacted the results of the 2016 United States Presidential Election and in the June 2016 Brexit referendum, the EU is cautious of the impact Russia could play in its internal dynamics if it is able to access citizens' data and disseminate disinformation among citizens of the EU. Furthermore, the rise of nationalism within the EU represents a push by Eurosceptics to cause further disfunction within the EU, which can be exploited by Russia to further diminish the centrality and influence of the EU (DeSilver 2019).

CONCLUSIONS

Clearly, the EU has acted in an expected way in its efforts for the protection of personal data and privacy. Examined through Power Transition Theory, the EU has successfully enacted the most progressive data protection regime in the world through economic regulation. Additionally, it is the security benefits of ensuring that individual's personal data and privacy are protected that will make efforts at using cyber tactics to disrupt the EU's influence more difficult. There seems to be immediate pressure from Russia flexing its capabilities in Ukraine, as well as exhibiting its influence worldwide through its interference with the United States 2016 Presidential Election. With the increase of the use of cyber-attacks and hybrid warfare, a rising Russia that is discontent with its international influence, and the accumulative reliance on technology in everyday life, the need for protecting data is ever apparent to the EU and its members.

The EU has clearly had its own struggles in unity, especially with the British decision to exit the EU, but its security remains paramount to its ability to function and ensure the economic competitiveness of its members. Although many EU members share membership in NATO, the EU has a need to ensure the economic security of its members and itself as the tactics being deployed by Russia to threaten the EU are nontraditional security concerns involving cyber tactics and data.

As international relations and power dynamics are constantly developing, it will remain important to keep a watchful eye on international events and the reactions by the international community. Only time will tell the success or failure of the EU. With the increasing prevalence in the use of hybrid warfare and cyber-attacks among states, along with the reliance on technology and data collection, the EU's early and progressive steps to protect its members' sovereignty and economic competition serve as a standard in the continuing development and enforcement of human rights law, extending to the right to privacy, and to data protection.

WORKS CITED

Aaronson, Michael, Sverre Diessen, Yves De Kermabon, Mary Beth Long, and Michael Miklaucic. "NATO Countering the Hybrid Threat." *PRISM* 2, no. 4 (2011): 111-24. https://www.jstor.org/stable/26469152

Bachmann, Sascha-Dominik, and Hakan Gunneriusson. "Hybrid Wars: 21st Centuryys New Threats to Global Peace and Security." *Scientia Militaria South African Journal of Military Studies* 43, no. 1 (2015): 77–93. https://doi.org/10.2139/ssrn.2506063

Boehme-Nebler, Volker. "Privacy: a matter of democracy. Why democracy needs privacy and data protection." *International Data Privacy Law* 6, no. 3, (2016): 222–229. https://doi.org/10.1093/idpl/ipw007

Council of Europe. *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, (1950). https://echr.coe.int/Documents/Convention_ENG.pdf

DeSilver, Drew. "'Euroskeptics' Are a Bigger Presence in the European Parliament than in Past." Pew Research Center. Pew Research Center, August 18, 2020. https://www.pewresearch.org/fact-tank/2019/05/22/euroskeptics-are-a-bigger-presence-in-the-european-parliament-than-in-past/

European Commission. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation." EUR-Lex. European Union, June 24, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

Fix, Liana. "The Different 'Shades' of German Power: Germany and EU Foreign Policy during the Ukraine Conflict." *German Politics* 27, no. 4. (2018): 498–515. https://doi.org/10.1080/09644008.2018.1448789

Giles, Keir. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power" Chatham House, March 21, 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-03-21-russias-new-tools-giles.pdf

Græger, Nina. "European Security as Practice: EU–NATO Communities of Practice in the Making?" *European Security* 4, no. 25 (2016): 478–501. https://doi.org/10.1080/09662839.2016.1236021

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal, January 2011. https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

IT GOVERNANCE PRIVACY TEAM. *EU General Data Protection Regulation (GDPR), Third Edition: An Implementation and Compliance Guide*. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2019. https://doi.org/10.2307/j.ctvr7fcwb

Kateryнchuk, Pavlo. "Challenges for Ukraine's Cyber Security: National Dimensions." Eastern Review (Łódź, Poland) 8 (2019): 137-47. https://doi.org/10.18778/1427-9657.08.05

Krishnamurthy, Vivek. "A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy." *AJIL Unbound* 114 (2020): 26-30. https://doi.org/10.1017/aju.2019.79

Kugler, Jacek, Ali Fisunoglu, and Birol Yesilada, "Consequences of Reversing the European Union Integration," *Foreign Policy Analysis* 11, no. 1 (2015): 45-67. https://doi.org/10.1111/fpa.12024

Lemke, Douglas. "The Continuation of History: Power Transition Theory and the End of the Cold War." *Journal of Peace Research* 34, no. 1 (1997): 23-36. https://doi.org/10.1177%2F0022343397034001003

Lemke, Douglas. *Regions of War and Peace*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 2002. https://doi.org/10.1017/CBO9780511491511

Limnéll, Jarno. "The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War." International Journal of Cyber-security and Digital Forensics 4, no. 4 (2015): 521-32. https://dx.doi.org/10.17781/P001973

Mueller, Robert S., *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* 2016. https://www.justice.gov/storage/report.pdf As used by the author from Peter Finn, Rosalind S. Helderman, and Matt Zapotosky. *The Mueller Report*. New York: Scribner, 2019.

Mundie, Craig. "Privacy Pragmatism," *Foreign Affairs.* February 19, 2014. https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism

Newman, Abraham L. "The EU Data Privacy Directive: Transgovernmental Actors as Drivers of Regional Integration." In *Protectors of Privacy: Regulating Personal Data in the Global Economy*, 74-98. Ithaca; London: Cornell University Press, 2008.

North Atlantic Treaty Organization (NATO). Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats. 25 August 2010. https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

Putin, Vladimir. Speech and the Following Discussion at the Munich Conference on Security Policy. 10 March 2007. http://en.kremlin.ru/events/president/transcripts/24034

Rosenbach, Eric, and Katherine Mansted. "How to Win the Battle Over Data," *Foreign Affairs.* September 17, 2019. https://www.foreignaffairs.com/articles/2019-09-17/how-win-battle-over-data

S. Rpt. 116-290. Senate Select Committee on Intelligence. Report, RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION Volume 4. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

Sanger, David E., and Nicole Perlroth. "Billions Spent on U.S. Cyberdefenses Failed to Detect Giant Russian Hack." The New York Times. The New York Times, December 16, 2020. https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html

"Shaping of a Common Security and Defence Policy." EEAS. European External Action Service, July 8, 2016. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5388/shaping-of-a-common-security-and-defence-policy-en

Simons, Greg, Danyk, Yuriy, and Maliarchuk, Tamara. "Hybrid War and Cyber-attacks: Creating Legal and Operational Dilemmas." Global Change,

Peace & Security 32, no.3 (2020): 337-342. https://doi.org/10.1080/14781158.2020.1732899

United Nations General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, 999, p. 171. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III). https://www.un.org/en/universal-declaration-human-rights/

United Nations, General Comment 16 from the "COMPILATION OF GENERAL COMMENTS AND GENERAL RECOMMENDATIONS ADOPTED BY HUMAN RIGHTS TREATY BODIES" HRI/GEN/1/Rev.1 (1994): 21-23. https://undocs.org/HRI/GEN/1/Rev.1

Voss, W. Gregory. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting." *The Business Lawyer* 72, no. 1 (2016): 221-34. https://www.jstor.org/stable/26419118

Walt, Stephen M. *The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy*. New York City, NY: Picador, 2019.

Weiss, Martin A., and Kristin Archick. *U.S. - EU Data Privacy: from Safe Harbor to Privacy Shield*. Washington, D.C. Congressional Research Service, May 19, 2016. https://crsreports.congress.gov/product/details?prodcode=R44257

Yakovleva, Svetlana. "Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?" *World Trade Review* 17, no. 3 (2018): 477–508. https://doi.org/10.1017/S1474745617000453