2014

German Foreign Policy in the Cyber Age

Patrick Schmitz

German Foreign Policy in the Cyber Age

Patrick Schmitz

Table of Contents

1. Introduction

The governance of cyberspace confronts states with traditional questions of sovereignty and identity: can they provide for their own security, or do they rely on the protection of other, more technologically advanced nations? Do they shape their identity in international security by following their own values or do they compromise their interests for the sake of cooperation? In the recent NSA surveillance scandal, these rather traditional questions have erupted in a new light. While appearing as a short-term security issue at first, the tension over surveillance has solidified the ways in which sovereignty manifests itself in cyberspace. A yet relatively unregulated space, the Internet possesses unique features such as the interconnectedness of users, the ambiguity of jurisdiction, and the accessibility of private information in a public domain. While all of these factors require an adaptation in defining state sovereignty in cyberspace, the NSA scandal has demonstrated that states project traditional, pre-existing values, and perspectives on the exercise of power onto cyberspace. This lack of adaptation in a new environment causes a long-term governance issue that will inevitably require more transparency and the defining of international norms.

The analysis of the NSA scandal through the lens of German foreign policy exemplifies this issue most eminently. Despite having gradually regained its sovereignty and identity in international security affairs in the post-war period, Germany took on a unique role in the scandal as the main target of the surveillance program (DW, 2013). Desiring a more independent position in security policy and valuing the protection privacy, the state finds itself in a transition phase in the transatlantic partnership: as Europe as a whole carries more weight in international security, the demand for U.S.

influence in European security policy has decreased (Zimmerman, 2005, 143). However, the lack of regulation and state legitimacy in cyberspace allowed the United States to enforce its values in international security and hold on to its desired scope of influence over European security. The dichotomy between intelligence and privacy—the security interests of the respective opposing sides—causes an irreconcilable governance issue. This dynamic demonstrates how pre-existing values and power structures in international affairs do not translate onto cyberspace. Instead, the clashes of opposing interests become intensified.

Threats and Sovereignty in Cyberspace

The diversity of actors in the Internet has complicated the definition of state sovereignty beyond the realm of territories. If not compromising state sovereignty, it has, at the least, raised questions over how sovereignty manifests itself in a yet largely "ungoverned" virtual territory (Nye, 2003, 68). The cyber age, therefore, presents new challenges for long-term governance.

The development of postwar Germany is an exemplary case of the traditional sense of sovereignty. German normalization, the broad term under which the regaining of sovereignty falls, represented a decline of external control over its foreign policy. A regaining of sovereignty also included rearmament and the dismissal of the occupation statute by the allies, a step that granted the German administration full control over its territory (Haftendorn, 2006, 15). German sovereignty also signified the legitimization of the newly arranged government, a factor that carries a lot of symbolic value (14).

Cyberspace complicates these traditional factors. The interconnectedness of actors operating online eliminates the territorial approach to defining sovereignty and jurisdiction. The resulting ambiguity of legal boundaries and the seeming absence of state control in the Internet complicate the physical manifestation and legitimization of state sovereignty. While governments employ architectural methods to symbolically represent sovereignty, private corporations take on a greater physical presence as they provide the services enabling the exchange of information. The transformation of private information into the public sphere, however, has extended the scope by which states can execute their sovereignty and security objectives. In this way, cyberspace limits sovereignty in its physical representation but facilitates its enforcement in security affairs.

This facilitation has raised the question whether cyberspace generates significant threats to national security. Advancements in technology have always influenced not only warfare and conflict but also the actors involved and the likelihood of conflict to occur (Andrews, 2012, 91). Cyber technology in particular has facilitated the means of warfare for a broader range of actors. Valuable targets such as government secrets, individual financial and personal information are more accessible than ever, as the Internet has dissolved the challenges brought forth by geography (91). Jurisdiction, physical security, and financial aspects have traditionally posed challenges to non-state actors in the security realm. The newly gained accessibility and ambiguity of jurisdiction have encouraged an increase in threats originating from non-state actors. In 2012, the Department of Homeland Security documented 198 cyber attacks targeting the information systems of private companies in several industrial sectors, a 52 percent increase from the previous year (Goldman, 2013). The attacks posed a security threat to

U.S. infrastructure, with the energy sector recording 82 of these attacks (Goldman, 2013). Most cases not only remain unreported but also unresolved (Goldman; Andres). Parallel to the rise of non-state involvement, states have increasingly used force in what James Adams called a "new international battlefield" in 2001. With over 30 states having invested in advancing their capacity for cyber warfare, nations now have the capability to attack the defense systems and infrastructures of foreign governments. Most notably, this strategy of virtual warfare was employed in Russia's invasion of Georgia in 2008 (Adams, 102; Reveron, 2012, 3).

While the new landscape of actors and online threats do not necessarily impact state sovereignty but rather require its adaptation, the act of cyber surveillance conducted by states brings forth more pressing questions on sovereignty. Particularly in cases in which surveillance does not represent an act of war but a preemptive security measure, a technologically advanced state can undermine the sovereignty of other actors by enforcing its security objectives at the cost of values and legal systems present in other states. Cyber surveillance, therefore, can be distinguished in the debate on cyber security and sovereignty.

The first chapter will focus on the ways in which sovereignty manifests itself in cyberspace and how states project their values in security onto this space. These themes spark the question of cyber security—does cyberspace generate a security risk? This question will solidify broader mechanisms of power and sovereignty that will eventually lead into the discussion of German foreign policy and current power constellations in transatlantic relations. This historical approach will help me analyze the ways in which traditional perceptions of power and sovereignty have manifested themselves in the NSA

surveillance scandal and the implementation of cyber security measures in the United States and Germany.

2. Sovereignty in the Cyber Age

Adapting Sovereignty

The emergence of cyberspace has caused a critical need to adapt our understanding of sovereignty. This question appears as urgent not only because of reasons linked to international security but also because of the long-term governance issue cyberspace entails. While the NSA scandal has brought forth the issue of cyber security, it has also demonstrated that the ways in which states approach cyber security has implications for civil liberties in a space lacking international norms. As sovereign states hold different values and implement different measures to ensure the civil liberties of their citizens, it is significant to understand how sovereignty is defined and manifests itself in cyberspace. In this way, the emergence of cyberspace has created a chain reaction: the exercise of cyber security by one state poses a threat to the sovereignty of another, undermining this state's security objectives and protection of its citizens' civil liberties. This dilemma in turn causes the need to reflect on sovereignty and collaboration through international norms in cyberspace.

Cyberspace complicates our understanding of sovereignty as a result of three distinct features: (1) the ambiguity of the legitimacy of power, (2) the interconnectedness of actors and resulting ambiguity of jurisdiction, (3) the accessibility of private information in a public domain. The analysis of these three components indicates that

cyberspace requires a redefinition of sovereignty and an adaptation of the ways in which states exercise their sovereignty in cyberspace.

Traditionally, the construction of sovereignty required the acknowledgment of implementing institutions, granting them the legitimacy to govern within a defined territory. In cyberspace, however, legitimacy remains more ambiguous than in the physical world. This ambiguity is created in part through the culture the Internet has produced. The wealth or even affluence of information, the ability to exchange this information with users throughout the globe, and the dissolving of physical boundaries have instilled a sense of illimitability and seeming absence of state power. Users of spaces offered by private corporations such as social media platforms have the ability to produce and individualize information. The major external entities setting the limits of and regulating this production are the corporations offering this space. The privatization of the Internet and its effective enabling of interconnectivity consequently seem to contradict regulation by governmental institutions. This contradiction is amplified by the difficulty in representing state sovereignty in a virtual world. While states employ physical representations such as monuments, governmental institutions, and other architectural symbols of sovereignty and legitimacy, the lack of such representations in a virtual space complicates the instilling a sense of legitimacy.

The virtual absence of the state in cyberspace also relates to the ambiguity of territory and jurisdiction. As the traditional definition of the sovereignty of states has heavily relied on territorial boundaries and jurisdiction, the interconnectedness of the Internet inevitably challenges this definition. International corporations such as social media sites or search engines host spaces for citizens to exchange information throughout

the world. Every information exchange can cross from one jurisdiction to the other. As some states such as China have enforced their jurisdiction by limiting or controlling their citizens' use of these spaces, others have remained in the background in regulating online information exchange. Both of these approaches come along with their individual sets of problems. A limitation of exchange of or access to information may undermine civil liberties such as freedom of speech. An unregulated cyberspace leaves citizens unprotected from criminal activity originating from domestic or foreign perpetrators. In the case of foreign perpetrators, the lack of territorial jurisdiction complicates their prosecution. Both foreign criminals and the intelligence services of other states can therefore attack or infringe upon the civil liberties of sub-entities of a state without crossing any territorial borders. While such infiltration into the territory of a state would have traditionally been defined as an undermining of state sovereignty and violated international law, the virtual nature of cyberspace complicates this traditional definition. The interconnectedness of users, therefore, suggests that jurisdiction cannot be enforced through clear territorial borders but requires an adaptation so that the international community can clearly define the infringement of state sovereignty in cyberspace.

The issue of shifting private information into the public domain pertains to the limitation of state sovereignty. The private, physical space occupied by citizens represents the limits of state sovereignty in many countries, manifesting itself in privacy laws in Europe or the Fourth Amendment in the United States, which prevents warrantless searches of private homes. Cyberspace has complicated the definition of privacy infringement as citizens occupy their own virtual space on the one hand but also publish their private information in a public domain. The absence of clear jurisdictional

boundaries, the fading distinction between the private and public sphere in cyberspace, and the technological capacity to access the private sphere of individuals across the world without the knowledge of the users have created the possibility that states widen and overstep the boundaries of their sovereignty that have traditionally limited them in the physical world. The accessibility of private information, therefore, sparks the debate over the scope of sovereignty in a virtual space that provides an affluence of new ways in which states can enforce their sovereignty.

Enforcing Sovereignty

The three ways in which cyberspace complicates traditional views on sovereignty consequently raises the question how sovereignty manifests itself in cyberspace. The NSA scandal showed that current governance of cyberspace is quite security oriented and that sovereignty manifests itself in the way in which states implement security measures to enforce their objectives. Two distinct ways have surfaced through this scandal and help explain security policy decisions in cyberspace: First, states enforce their sovereignty based on their perception of security threats, which originates from underlying values in international security. Second, states attempt to maintain pre-existing power structures and maximize their autonomy in cyberspace.

The definition and perception of security threats in cyberspace has remained ambiguous and varies across different nations. This ambiguity seems to have instilled uncertainty and fear, resulting in exaggerated security measures. As the perception of threats depends in part on cultural factors, sovereignty manifests itself in the ways in which states project their values onto cyberspace and enforce these values in their

treatment of data and information. States that value the protection of privacy, for instance, perceive an infringement of privacy as a security threat and will implement policies accordingly. States that value a strong governmental presence in shaping political culture will perceive the exchange of and access to certain information as a security threat and take a more proactive approach to limiting these uses of the Internet. States that value the physical protection of their citizens will perceive information exchange as an opportunity to oversee communication and prevent possible acts of terrorism. In all of these cases, the ambiguity of the virtual space has the potential to create fear and uncertainty: to what extent does technology enable actors to access private information? What is the potential of information exchange and knowledge with regards to political activism? Do extremist groups have the technological sophistication to facilitate or even execute terrorist attacks in cyberspace? As these questions raise even more uncertainties, the NSA scandal has demonstrated that states tend to compensate for a lack of knowledge through extensive and proactive security measures.

Simultaneously, these security measures pertain to the maintenance of power and ways of governing. While the protection of privacy, the control of information exchange, and the gathering of information or intelligence purposes have always played a role in exercising state sovereignty, cyberspace has intensified the scope by which these measures have to be carried out: privacy pertains to a broader range of actors and data, information exchange occurs on a more frequent and interconnected basis, and security-related information is increasingly accessible. Maximizing the capacity and autonomy by which these measures can be implemented, states attempt to maintain pre-existing ways of exercising power in a space that intensifies the clash of security objectives. In the NSA

case, for instance, the United States projected its military power onto cyberspace and maintained its pre-existing leadership and autonomy within the transatlantic partnership. The gathering of data represented the major tool of this militarization and enforcing of U.S. sovereignty.

A Need for Surveillance?

The emergence of information technology has added a wide range of problems to ensuring national security (Gravelle, 2012, 111). As many opportunities as the Internet provides to corporations and Internet users, it also provides opportunities to extremists and hackers. The unique characteristic of cyberspace is the simplicity of access. While other realms of operation for terrorists require financial investment, cyberspace requires only technological knowledge and devices that connect to the Internet (Reveron, 2012, 7). The infrastructures of the state and the energy sector, bank accounts of private individuals, operating systems of government agencies, and data stored by large corporations are directly accessible and vulnerable targets to a wider range of actors (11). In fact, individuals and non-state actors conduct most malicious activity on the Internet while some attacks can be traced back to government-sponsored programs (11). The wide range of actors and unlawful actions in cyberspace complicate the definition of cyber terrorism and its threat to international security. However, the NSA surveillance scandal has uncovered the existence of both incentives for states to conduct cyber surveillance and differences in the values and priorities they project onto cyber security programs. It

has raised the question whether these incentives originate from real threats and opportunities.

The definition of cyber terrorism has derived from a wider spectrum of uses of cyberspace for illegal purposes and is more ambiguous than the definition of cyber warfare (Awan, 2012, 23). Timothy Thomas notes that the "Naval Postgraduate School (NPS) has defined cyberterrorism as the unlawful destruction or disruption of digital property to intimidate or coerce people" (Thomas, 2003, 112-13). Similarly, scholars such as Gabriel Weimann (2004) see cyber threats as generally unlawful means to attack the infrastructures of states, including cyber terrorism in the wide spectrum of illegal activities occurring in cyber space (Stohl, 2007). According to Imran Awan, however, there needs to exist a differentiation between cyber terrorism and cyber crime—a necessary distinction to separate the very pressing issue of cyber crime from the yet ambiguous concept of cyber terrorism (Awan, 33). Michael Stohl concludes that the definition of cyber terrorism needs to align with traditional views of terrorism and defines it as, "The *purposeful* act or the threat of the act of *violence* to create *fear* and/or compliant behavior in a *victim* and/or *audience* of the act or threat" (Stohl, 2007). With this definition, Stohl maintains the "effects-based" approach but emphasizes that the intention behind an attack characterizes it as an act of cyber terrorism (Stohl, 2007). In a testimony before the Committee on Armed Services in 2000, Dorothy Denning defined cyber terrorism as, "the convergence of terrorism and cyberspace" (Denning, 2000, 1). Like Stohl, she stresses that, "to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water

contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (1). All of these different definitions solidify the question whether cyber terrorism poses a real threat to governments.

While scholars are aware of the organizational uses of cyberspace as described by Timothy Thomas and Gabriel Weimann, they are more skeptical about the existence of cyber terrorism based on Denning's definition. In fact, Michael Stohl argues that cyber terrorist attacks with severe outcomes have not yet occurred (Stohl, 2007). Even though Denning mentions several instances in which politically motivated hackers have caused severe financial and material damage in the past, she acknowledges that the concept of cyber terrorism is "mainly theoretical," as none of the attacks have caused any physical harm to civilians" (Henning, 1-2). However, she speaks of infrastructural vulnerabilities terrorists, if acquiring the technical knowledge, could potentially use to their advantage. This speculative view of cyber terrorism is what Imran Awan calls the "Doomsday Scenario," according to which terrorists would employ cyber technology to cause airplane crashes or to take charge of missiles and bombs (Awan, 24). Despite the speculation about terrorists' technological capabilities in cyberspace and the threats against which states are vulnerable, the Internet seems to have great value to national security. At the very least, scholars have argued, the Internet offers terrorists an operational structure, which facilitates the execution of attacks in the physical world.

Consequently, scholars have engaged in a discussion over how terrorists use the Internet. Maura Conway argues that the wide range of uses to which scholars such as

Fred Cohen (2002), Timothy L. Thomas (2003), or Gabriel Weimann (2004) have referred fall under five overarching categories: "information provision, financing, networking, recruitment, and information gathering" (Conway, 2005, 3). In some respects, these uses of cyberspace by terrorists seem to align with the ways in which other non-state actors such as hackers and criminals operate. While cyber crime has existed in the form of malicious activity such as identity theft or the disrupting of governmental and corporate networks, cyber terrorism can appear in similar actions that are motivated by political or ideological agendas. In this context, terrorists have also employed the Internet for propaganda, networking, recruiting, and training of new members. Websites of extremist groups contain messages, forums, and videos furthering the cause of their political beliefs. While these uses of cyberspace do not directly represent terrorist acts, they are closely linked to the organizational structure and execution of terrorist acts in the physical world (Awan, 23-31). There exist, however, more direct ways in which terrorists can employ cyberspace for the execution of terrorist acts. During the September 11 attacks, for instance, terrorists used encrypted messages to communicate with each other, laying the foundation for their attacks (Awan, 28). In recent years, the concern over direct terrorist attacks through cyberspace has grown in the intelligence community. While hackers without political agendas have managed to disrupt infrastructures or corporate networks in the past, the British intelligence agencies, for example, have voiced their concern over a rise of terrorism through similar cyber attacks (Awan, 21).

The main concern of the intelligence community is what Timothy Thomas calls "cyberplanning"—"the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed. It can include

cyberterrorism as part of the overall plan" (Thomas, 2003, 113). This definition pertains especially to the organizational means of Internet services. Conway's five uses broadly categorize instances of cyberplanning. Information provision includes the spread of messages to a broad audience that may serve propaganda purposes or even psychological warfare, instilling fear of the capabilities of terrorist organizations (5). The videotaped executions of Nick Berg and Daniel Pearl in the early 2000s are two examples (5). The spread of messages usually takes place through websites affiliated with extremist groups. These websites often provide opportunities for fundraising as well: they target specific visitors and potential donors through encrypted messages (6). In some cases, extremists attract unknowing donors through fake websites of charities that claim to follow peaceful intentions (Thomas, 2003, 116). In this way, much of the funding systems remain invisible to intelligence agencies.

Terrorists employ similar techniques to recruit new members (117). As propaganda occurs in a public manner, potential members may become attracted to extremist views. With regards to networking, Conway observes that the use of online communication is causing the decline of hierarchical structures within terrorist organizations: sophisticated undercover communication systems enable the decentralization of power and a shift towards network-like power structures (Conway, 10-11).

While terrorist communication remains mostly unnoticed, extremists make use of publicly available information: in 2003, "Defense Secretary Donald Rumsfeld observed that an al Qaeda training manual recovered in Afghanistan said, 'Using public sources and without resorting to illegal means, it is possible to gather at least 80 percent of all

information required about the enemy'" (Thomas, 118). This information may include infrastructural or architectural features of potential targets, as demonstrated by an al Qaeda computer containing information of a dam with which engineers could plan a possible attack more efficiently (118).

All of these uses facilitate the coordination of terrorist attacks in the physical world and incentivize governments to establish measures to gain valuable information on terrorist activity. Yet, these uses merely represent indirect links to terrorist attacks. As argued by most scholars, cyberspace does not yet pose a security threat in itself. The answer to the question whether there is a need for surveillance or not, therefore, depends on interpretations, values, and psychological effects the perceived threat of cyber terrorism imposes on administrations and how these factors manifest themselves in the institutional and legal structures of national security. However, the NSA scandal has indicated an exaggeration of security measures in the United States and shows the currently imbalanced and inefficient approach to governing cyberspace.

As a consequence, states apply pre-existing, traditional perceptions of power and sovereignty and values in international security onto a space that requires a redefinition of these terms. The transatlantic relationship, German-American relations in particular, have solidified this dichotomy. The evolution of German foreign policy—Germany's reemergence from a semi-sovereign status to a major actor in international security—and its close link to American security policy outlines the pre-existing perceptions of sovereignty and power that incentivized the construction of sovereignty in cyberspace. The clash of identities and values in the German-American case exemplifies the impossibility of the traditional exercise of power in cyberspace.

3. The Evolution of German Foreign Policy

The Way to Sovereignty

In August 1949, the Federal Republic of Germany held its first elections. With Theodor Heuss as the federal president and Konrad Adenauer as the first chancellor, the elections marked a first step towards autonomy. This first step, however, came along with a set of conditions: the Allies would maintain jurisdiction through an occupation statute, which granted them control particularly on the foreign and security policy front (Haftendorn, 2006, 15). On September 21, 1949, representatives of the allied states came together in Bonn to present the occupation statute to Adenauer. The planned formality of this ceremony and its actual outcome symbolized the integration process of the Federal Republic into the West (Haftendorn, 14). While the commissioners had restricted Adenauer from joining them on the red carpet before the chairman's official declaration of the statute, the chancellor skillfully bypassed this rule, as he recounts: "I went up to the Petersberg in the company of a few federal ministers. We were led into a room where we were received by the three High Commissioners standing on a carpet. Francois-Poncet was chairman that day. While I stopped in front of the carpet he took one step forward to greet me. I saw my opportunity, went towards him and thus stood on the carpet myself. None of the High Commissioners objected. Francois-Poncet gave his speech" (Haftendorn, 15). Adenauer's account represents the larger picture of German integration into the West; the idea that the allies would cease formal provisions within the context of reconciliation, economic rehabilitation, and common security objectives.

The reemergence of Germany as an autonomous actor in international security has, therefore, largely been an extending of its scope of action with regards to Europe and the United States. The end of World War II and the founding of a West German state in 1949 represented the beginnings of a "Road to Europe" on the one hand and the establishment of an "Atlantic Alliance" on the other (Haftendorn, 83). The regaining of sovereignty seems to have paralleled these two processes, taking place under foreign supervision and marked by various key events leading up to reunification in 1990. The presentation of the occupation statute to representatives of the Federal Republic implied that, despite the founding of a new German state, the nation had not regained sovereignty immediately after the war (Haftendorn, 14). German rearmament eventually indicated a first step towards sovereignty. The question of rearmament solidified differing goals and priorities for the parties involved: for Chancellor Konrad Adenauer, rearmament meant a basis for sovereignty, counterbalancing armament in the East, and an institutionalization of European military forces. Cautious about a potential rise of Germany as a major military power, France objected to Germany's entry into the NATO. The United States, pushing for this entry, sought to strengthen Europe's military force and eventually reached a compromise for Germany to contribute outside of the NATO realm (Haftendorn, 23, 26). This compromise between national and international interests in the establishment of the European Defence Community (EDC) Treaty of 1952 demonstrated that Germany's recurring pursuit of autonomy could take place only within the context of European institutions. This rather self-contradictory fact was enforced in the General Treaty of 1955 that initially granted the state its partial sovereignty: the United States,

France, and Britain maintained certain rights for influence in Germany and, with them, the state's "semi-sovereign" nature until 1990 (Wittlinger, 13, 2013).

The EDC Treaty and the General Treaty lead to opposition on the German domestic stage and revealed a general aversion to militarism: the culture of postwar German foreign policy was marked by a sense of overcorrection, to counteract the former striving for power (*Machtversessenheit)* through self-restraint and even an "oblivion of power (*Machtvergessenheit)*" (Wittlinger, 13). This conscious shift in approaching foreign affairs contradicted the security needs of the republic's allies. Germany's entry into the NATO in 1955 further complicated this contradiction. The lack of domestic support for rearmament was complemented by an abundance of responsibilities towards a variety of critical partners and regions, a dilemma posed by the central location of Germany in Europe. NATO membership brought forth three distinct but opposing roles that Henning Tewes described as influences on German priorities in international security: the "Atlanticist" role emphasized on Germany's responsibility to enforce U.S. security interests while the "Gaullist" approach would prioritize a pivot towards Europe (Tewes, 2002, 7). These two objectives intertwined in Germany's military and economic integration into the West (*Westbindung).* The "Muscovite" role, however, indicated a need to refocus foreign policy towards the East, a route taken in Chancellor Willy Brandt's *Ostpolitik* (Tewes, 7).

Between Transatlantic Relations and European Integration

Germany's reemergence on the international stage has demonstrated two major mechanisms that have resulted in the challenges and opportunities of transatlantic

security in the present. First, Europe has become more integrated. As established in the previous section, this integration commenced on the foundation of economic and security interests and specialized institutions and has now evolved as a broader, overarching cultural and political institution. While Germany has gained its full sovereignty, it has gained it under the condition of integration. This new interconnectedness comes along with mutual responsibilities in the security realm. Second, the integration of Europe and full sovereignty of Germany has decreased the functionality of U.S. influence in European security affairs (Zimmerman, 2005, 143). While Germany carries emerging responsibilities towards European institutions, it has faced the challenge of balancing these responsibilities with the interests of its symbolic and historical partnership with the United States. This balancing is complicated by the observation that the two mechanisms have caused irreconcilable values and priorities in international security between Europe and the United States to be more likely to surface. These conditions have intensified the diplomatic crisis over NSA surveillance programs.

As analysis in Chapter 4 will show, the NSA scandal has confirmed the remaining existence of these mechanisms. Even though the Internet poses a security concern for both, the United States and European countries, contradicting definitions of threats and different priorities have polarized both sides on the issue. While Germany's security priority—the protection of privacy—aligns with the priorities shared with the rest of continental Europe, the United States has militarized cyberspace as a response to perceived cyber security threats by terrorist groups. The exaggeration of U.S. policies pertaining to the regulation of the Internet has continued the trend of conflicts of the last two decades that have demonstrated an irreconcilable American exceptionalism in

involvement in European security. Before analyzing the diplomatic and policy background of this recent scandal, I will expand on the debates on Germany's foreign policy trends and the mechanisms surrounding its relationships with European institutions and the United States. This analysis will place the recent cyber surveillance issue within the broader context of transatlantic relations and European integration.

Out of the two mechanisms described above grew several theories about the nature of the new unified German state. Debates focused on the ways in which the context of intergovernmental institutions, the presence of the past, and national identity had shaped Germany's foreign and security policy objectives. Would Germany take on greater responsibilities and how would it prioritize its obligations towards the United States and Europe? Were there incentives for a new sense of German exceptionalism? In analyzing the reconstruction of post-war Europe, optimists have projected the image of "a Germany tamed by international ties" (Markovits; Reich, 1997, 44-45). This conclusion is grounded in arguments ranging from Germany's collective memory and prevention of future abuses of power to economic interests in European integration and the impossibility of a sustainable balance of power in a disintegrated Europe (44). These arguments consider the European Union as an institution constraining the use of power and, more importantly, an institution incentivizing Germany to prioritize economic growth over relative power.

While the pessimists acknowledge Germany's legal obligations to intergovernmental institutions, they believe that these multilateral structures serve as a new ground for German exercise of power (Markovits; Reich, 50). They argue that the introduction of a European-wide currency happened on the terms of German interests:

specific requirements on state debt, for instance, suited only the already dominant state of the German economy (51). In addition, they refer to a report by CDU / CSU parliamentary leader Wolfgang Schäuble who noted that Germany and France were to fuel the project of European integration, with all other countries having to adapt to the standard of economic progress imposed by the core states (51). The pessimists believe, therefore, that the new structural and economic landscape of Europe allows Germany to redefine its control over its neighbors—the desire of power still exists and the Federal Republic has found new ways of channeling its exercise in peaceful ways (52). Along with economic power, the state has increasingly exercised cultural power in Eastern Europe, a newly accessible territory for German influence (50).

In the realm of competing theories in international relations, the perspective of Germany as a civilian power had gained increasing popularity leading up to and immediately following reunification (Dettke, 2009, 5). Hanns W. Maull, one of the most prominent advocates of this theory, referred to the "'civilising' of international relations," the process by which nations project domestic democratic values onto international organizations and regimes (Harnisch; Maull, 2001, 3). The theory is closely linked to liberalism—it anticipates the need for regulating individual state sovereignty as states increasingly rely on multilateral agreements to protect themselves (Tewes, 10-13). As a consequence, it values the creation of interdependent and cooperative security communities in which military force serves merely self-defense or the promotion of democracy—two concepts that may cause several contradictions (Tewes, 12). This last point resolves, however, the commonly held belief that the civilian power paradigm is a pacifist one (12). The multilateral approach to security in this argument assumes that a

state would forgo national interest or even its sovereignty for the objective of civilizing international systems (Maull, 4).

This process has been, according to its supporters, the driving force behind decision-making in German foreign policy. Since reunification, several foreign policy issues have been at the center of focus, ranging from Germany's work on nuclear nonproliferation to its stance on Kosovo, Afghanistan, and Iraq. In general, supporters of the civilian power theory such as Andrei Markovits and Simon Reich point to the fact that Germany abstained from responsibility in security affairs despite its significant economic power, redefining the concept of German exceptionalism (Markovits; Reich, 1997, 206). The exceptionalism of the Third Reich derived from its exercise of power in Europe; the one of the post-war period, on the contrary, marked a willful neglect of power and a shifting of responsibility towards the international stage (Markovits; Reich, 206).

Markovits and Reich's argument gains significance particularly with regards to the early stages of German militarism after unification. The question of German involvement in the First Gulf War brought forth several contradictions in the nation's use of force and its relationships with its allies. Nina Philippi points out that Germany, focusing on growing the economy of the unified state, had not yet acknowledged the rise of new types of security challenges after the fall of the Soviet Union. The idea of smaller military operations had been undermined by the fear of another world war, leading foreign policy experts to condemn the use of force in Iraq (Philippi, 2001, 50-51). At the same time, the voices against the Gulf War on the domestic front were mainly targeted at the international community and meant to establish Germany's open aversion to military

use (51). Even though nations such as Israel and France had previously feared and opposed German rearmament, they now condemned the state's passiveness in Iraq and questioned its commitment to the security community (52). Philippi argues that especially Germany's opposition against military use in Iraq and general hesitation leading up to Kosovo complicated Hanns Maull's depiction of Germany as a civilian power (63f.). In reference to Germany's secondary role in Western security affairs, she argues that, "an ideal type Civilian Power would not always stand in the second row but be a global player who actively tries to foster its civilising tasks . . . The 'power-element' within the Civilian Power model is therefore underdeveloped" (65).

The debate over the Gulf War in 1990-91, therefore, demonstrated the contradiction within the civilian power stance for Germany: cooperation often contradicted domestic values regarding security and Germany's integration into international organizations would be complicated through the changing security demands of the international community. The Gulf War case also demonstrated a shift in international expectations. Philippi's argument shows that the reconciliation of World War II could not occur simply through German pacifism and a commitment to self-defense in the realm of NATO. Instead, Germany was increasingly expected to match its economic power in security matters, an observation that aligns with Markovits and Reich's statement on a new German exceptionalism. Rather than holding on to a pacifist stance, Germany would have to reconcile its past through a commitment to its allies' security objectives, regardless if this commitment came in the form of military contribution. Germany's reemergence as an actor in international security consequently required the adaptation to a new international order and a redefinition of how the nation

would reconcile its past. These changes meant that the administrations had to undermine existing cultural values and overcome contradictions on the domestic front to effectively integrate into a cooperative security community.

Despite these challenges in German foreign policy, supporters of the Civilian Power model applied their theory to interpret the nation's decisions in international security. Henning Tewes, for instance, argues that NATO enlargement in 1994 exemplified a case of German civilian power: the administration supported the inclusion of Eastern European states into NATO under the condition that it would not impair Germany's relationship with Russia (Tewes, 2001, 19). The spread of democracy presented the main incentive for enlargement, demonstrating the nation's interest in incorporating its democratic values in intergovernmental organizations (19). This careful consideration of both cooperation with Russia and broadening the scope of NATO as not only a security but also democratic community seemed to highlight Germany's role as a civilian power (20). However, this rather cautious approach can also be interpreted as a balancing of conflicting national and international interest and an internal debate over Germany's identity in security affairs. The enlargement of NATO represented further integration of security ties in Europe—an idea the United States generally supported. The acknowledgment of cooperation with Russia, which was grounded in economic interests, showed the dichotomy of Germany's simultaneous reemergence in the global economy and international security. The civilian power model, in this case, relies too heavily on the idea of sacrifice for the sake of integration and cooperation. It overlooks the idea that conflicting economic and security interests shaped the contemplation over NATO enlargement.

The contradictions brought forth during the period of the First Gulf War and NATO Enlargement debate manifested in the question on a normalization of German power. The civilian power perspective had dominated this question—its link to liberalism and support of the idea that Germany would not follow its national interest in security affairs lead observers to believe in a remaining German exceptionalism. Germany's pacifism and unwillingness to take on greater responsibilities only perpetuated the view that Germany had not been normalized. The false interpretations of the civilian power model as a pacifist one made it seem irreconcilable with normalization.

Military intervention in Kosovo posed a first step to reconciling this conflict. While critics argued that German military intervention in Kosovo was a reaction to outside forces—the United States had pressured the newly elected administration under Chancellor Gerhard Schröder and Foreign Minister Joschka Fischer into a quick decision—Hanns Maull attributes German involvement to a combination of domestic and international forces. While international expectations did pressure Germany into taking action, the administration had its own agenda in making a decision in favor of the use of force (Maull, 2001, 118). First, Germany had an interest in maintaining the legitimacy of the international institutions involved. Having learned from the experience of the first Gulf War and since developed an open-mindedness for military force, the German public increasingly accepted Germany's commitment to NATO, the EU, and the UN through the use of force; a development that gave Schröder and Fischer the domestic support to act instantly (Maull, 117). Second, Maull argues that "deeply held beliefs and norms" about Germany's responsibility to prevent further genocides made intervention in Kosovo indispensible (118). He concludes that, despite the shift towards military use, Germany

strengthened its positions as a civilian power as it projected its democratic values onto cooperation within international institutions (120).

Maull's reliance on underlying norms and values becomes problematic in light of the inconsistency in German foreign policy decisions. Following Germany's abstention to provide military aid to Libya, The Economist published an article titled "The unadventurous eagle" in 2011, noting that the central European country was alienating itself from its traditional allies in Europe and across the Atlantic. The author argued that the nation entered a new trend of following German exceptionalism, no longer being invested in its multilateral agreements and former partnerships. Hanns Maull contributed with the observation that Germany lacked a "grand strategy" (Economist, 2011). Since this alienation posed an issue since the first Gulf War, it is arguable that the concept of German exceptionalism is a recent development. Yet, the inconsistencies in foreign policy decisions seem to support the idea of exceptionalism and complicate the civilian power model. If Germany were still or had ever been a civilian power, would it not have developed a clear "grand strategy"? In fact, the civilian power paradigm represents a grand strategy in itself. Germany's inconsistencies, therefore, prove the theory as insufficient in fully explaining the nation's foreign policy behavior.

Normalization, Sovereignty, and Transatlantic Relations

The civilian power theory had persisted throughout the postwar period and the first decade after unification because German values and public interest largely aligned with the integration into the West and development of multilateral agreements. Germany's recent alienation from its allies has revived arguments of a special path and

the country's inability to form long-term alliances. To some, however, this alienation does not represent a special path for Germany. Instead, it renders support to the idea that Germany has become a normal power.

Normalization in international affairs, specifically in the case of Germany, has been subject of change and multiple different definitions (Dettke, 21). Since the end of the Second World War, international expectations of German reconciliation have put the issues of reparations and responsibility for war crimes at the center of normalization. In this context, normalization required reconciliation with Germany's neighboring countries, former Soviet nations, and the support of the autonomy of Israel. According to Dieter Dettke, reconciliation was a problematic definition for normalization: while Germany demonstrated its willingness and efforts for reconciliation through reparations and compensation programs, the insufficiency of these concessions to reconcile the past would indicate that Germany would "remain imprisoned in its past" (21). Even the idea of pacifism did not provide an adequate moral standard for reconciliation as both military actions as well as inaction entail ethical problems (21). The evaluation of normalcy, therefore, had to reach beyond the complicated boundaries of reconciliation.

As post-war Germany was a semi-sovereign state, the regaining of sovereignty and reemergence as an autonomous actor in international relations play a significant role in defining normalization. Germany's and particularly Chancellor Gerhard Schröder's campaign against the Iraq War in 2002-03 has become a major point of contention with regards to this reemergence. Some projected the Civilian Power model onto the decision to abstain from the use of force in Iraq—the decision demonstrated the country's hesitation regarding out-of-area operations and reconfirmed its striving for a special path

and a commitment to pacifism (Zimmermann, 2005, 128). Germany's goal of building a coalition in the U.N. Security Council that would serve as a counterbalance to American influence seemed to support this perspective. However, Dieter Dettke argues that the stance taken by Chancellor Schroeder's administration was rooted in the principle of following national interest and autonomy (Dettke, 7).

While many realist scholars saw the German-American tension over Iraq as a long-lasting division between German and American security policy, Dettke argues that based on modern realism, particularly defensive structural realism, Germany's more aggressive behavior in following its national interest does not necessarily imply a structural alienation from the United States or Europe. Instead, it "anticipates that hard-line policies focusing on political and military competition lead to self-defeating consequences" (Dettke, 14). This argumentation implies that nations maximize on their ability to enforce their own policies but acknowledge the limits presented to them by the structures of power and multilateral agreements. The debate over German normalcy thus also includes the question whether normalization would mean the end of German-American relations or German-European relations as they have existed since the end of World War II.

Other evaluations of normalcy focus on policy-interests and the specific roles states take on to exercise these interests. Hubert Zimmerman, for instance, argues that Germany's reemergence on the international stage has brought forth a new dynamic in German-American relations:

> "To an extent unprecedented in the postwar era, Germany and the United States now pursue structurally similar international policies. Since the end of the Cold War, Germany has become an *exporter of security* abroad, whereas previously it had been an *importer of security* from the United States. Thus the fundamental

> policy objectives and policy tools of the United States and Germany in the international system are becoming more alike, as both seek to address security threats by intervening abroad – politically, economically, and militarily" (Zimmermann, 129).

This theory relies on a historical evaluation of the evolution of German foreign policy. The global power structure in the post-war era caused the necessity and, consequently, the acceptance of American hegemony in security policy in Europe. The counterbalancing of Soviet power, in Zimmermann's terms, represented a "burden-sharing" that exceeded the boundaries of international security—it pertained to the economic, political, and arguably the cultural development of the Western alliance. The concept of "importing" or "consuming" security is based on a business-related model that indicates an exchange of security and protection on the one hand, and an acknowledgment of leadership and long-term hegemony on the other. The factor of sovereignty plays an important role in this exchange. The acknowledgment of U.S. hegemony specifically in Germany represented an acknowledgment of the semi-sovereign nature of the West-German state. American hegemony meant military presence in Germany and throughout Europe and special rights of oversight of German foreign and domestic policy by the allies. While this oversight, as previously discussed, decreased in formality, it remained in the way of a complete reemergence—or normalization—of German foreign policy until the end of the Cold War, which arguably marked the end of the European need for American protection. Accordingly, for as long as Germany remained an "importer of security," sovereignty was dispensable—the business model presented a fair solution to the "burden-sharing" in the West.

Zimmermann's theory also suggests that normalcy is measurable by the degree to which a country's policy interests and their enforcement align with the general foreign

policy behavior and consensus of other states within its alliance. In the case of Germany, Zimmermann refers to its use of military force in the Kosovo War; a decision that marked the beginning or a first major test of Germanys "exporter role" in international security, though preceded by several smaller steps of intervention and stabilizing measures in the area (141). Over the years, Zimmermann argues, the European Union had played a key role in stabilizing Eastern Europe with the export of security to Bosnia, Kosovo, and Macedonia, resulting in a transformative foreign policy role for the union as a whole (141). Germany showed its leadership in providing stability in these particular regions despite the rather limiting perspective of the civilian power theory. Zimmermann concludes that Europe's and Germany's leadership in Eastern Europe has transformed the role not only of Europe but also of the United States: if more European countries demonstrate their capacity to provide stability, "the functional basis for asymmetrical US leadership of the Atlantic partnership is gone" (143).

These observations suggest that the transatlantic relationship finds itself in a transitional phase in which European powers, including Germany, have achieved normalcy through "exporting" stability. The challenge of this transitional phase, according to David Andrews, is a newly gained sense of freedom by which the United States determines its actions. During the Cold War, the constant threat of the Soviet Union required a unified counterbalance of power in the West. Even though the United States took on the leadership role of exporting security to Europe, it relied on the support of European states in security affairs. The crisis in transatlantic relations of the last decade, initiated by the War on Terror and the Iraq War in 2002, has demonstrated that the United States no longer depends on long-term support from its European allies

(Andrews, 2005, 69). At the time the United States began its course of fighting terrorism and lobbying for international support, U.S. Secretary of Defense Donald Rumsfeld spoke of "'floating coalitions of countries'" and stated that, "'the mission will define the coalition – not the other way around'" (Zimmermann, 144). With this statement, he contrasted the current constellation of U.S. allies with the long-term partnership that was once formed for a common overarching goal. The statement also shows the willingness of the United States to act upon the newly gained freedom of building short-term coalitions and even face the risk of enforcing national interest by itself. Addressing the recent surveillance scandal, Henry Farrell and Martha Finnemore refer to the United States as a "hypocritical hegemon" whose policies have often been tolerated and legitimized because of the international system and values it has generated in the last century (Farrell, Finnemore, 2013, 2). Hypocrisy, in this context, has been an essential tool for the United States to operate within this system (2). This argument confirms the idea that the United States can no longer rely on support from its allies based on its higher moral ground. Instead, there needs to exist a real incentive for cooperation between the U.S. and its allies who decreasingly "benefit from the global public goods Washington provides" (3). The transitional phase of the transatlantic relationship is consequently characterized by a disconnect between the lack of functionality of U.S. influence on European security policy and the sense of freedom of the United States to enforce its policy interests in short-term coalitions.

The cyber surveillance scandal and the relatively new challenge of cyber security have confirmed the existence of this disconnect. While states—including Germany—have an interest in using cyberspace as a means of security, there is a lack of equality in

determining the extent to which they should regulate and control data. Additionally, direct threats in cyberspace—especially terrorist-related attacks—have not yet been as pronounced to incentivize and legitimize the degree of protective measures the United States has implemented. Having put these surveillance programs in place, however, the United States has acted upon its ability to follow its national security interests without seeking long-term coalitions. The lack of transparency in cyberspace has facilitated this process. Regardless of the extent to which other states such as Germany were aware of the program, the United States has acquired the technological capacity to establish its hegemony in a shared space.

The business model of importing security and acknowledging hegemony therefore no longer adequately addresses the circumstances of power and roles from a European perspective. The scandal has brought forth clear objectives and values European states, especially Germany, are aiming to project onto their regulation of cyberspace. Sovereignty, with regard to cyber surveillance, manifests itself not only in the control of data but also in the degree to which states can enforce their values onto regulation of the Internet. The United States has, in Farrell and Finnemore's terms, exercised its sovereignty by enforcing its values in international security in a yet relatively unregulated and largely undivided space and thereby undermined the sovereignty of others. In this case, however, strongly held values and sensibility regarding privacy and data protection make the exchange between sovereignty and protection too costly.

With regard to normalization, the cyber surveillance case has solidified the idea that German normalization—a more leveled playing ground in international security—is inevitably linked to the United States. The mechanism of Germany's reemergence as an

autonomous actor and simultaneous decline of American influence on its security policy implies a remaining German dependence on the United States: even though Germany has reestablished itself as an "exporter of security," and taken on new roles and responsibilities since reunification, the United States has maintained its expectation of the transatlantic relationship—that it provides security for the price of hegemony. The final step in German normalization consequently depends on a redefinition of the role of the United States in transatlantic security. In the following chapter, I will analyze how the new dilemma of sovereignty and American hegemony in transatlantic relations has revealed itself in the diplomacy- and policy-related issues of the NSA scandal.

4. Germany and Cyber Security

A Symbolic Scandal

When Edward Snowden leaked information on surveillance programs conducted by the NSA in 2013, the transatlantic relationship was already facing several ongoing challenges. The scandal threatened to interrupt ongoing and already contentious talks on a free trade agreement between the United States and the European Union called the Transatlantic Trade and Investment Partnership (TTIP). As the United States and Germany had previously experienced tension over German military action in Libya, to which the German government abstained despite pressure from both the United States and Europe, they now faced a similar situation with regards to Syria. U.S. Secretary of State John Kerry and German Foreign Minister Guido Westerwelle disagreed on the question of providing arms to Syrian rebels, with Mr. Westerwelle remaining cautious

and suggesting to follow the course of the conflict. Despite their collaborative diplomatic measures against the Russian government, which stood in the way of peace talks in Syria, their disagreement added to the recurring tension in transatlantic cooperation in international security. On top of these points of contention, which had occurred in a long string of events leading to alienation on both sides, the summer of 2013 was of historic and symbolic significance—it marked the 50th anniversary of President Kennedy's speech in Berlin in 1963. In commemoration of the speech that most explicitly tied the people of Berlin and Germany as a whole to the guiding values and worldview of the United States, President Obama was invited to speak in Berlin in June 2013.

In the midst of all these circumstances, the surveillance scandal combined several significant facets and layers of contention in German-American relations and solidified core issues pertaining to cultural and political values, economic aspects, and the question of leadership in security affairs. Even though cyber surveillance and data privacy will continuously impose an important policy challenge on these countries, the NSA scandal by itself appeared first and foremost as a symbolic scandal, representing deeper fundamental challenges to be overcome in the future. The progression of the scandal—the interaction between different levels on the German domestic front and their changing reactions to the revelations—has demonstrated this observation. The neutrality and silence of Merkel's administration contradicted the public outrage at first. Having relied on rather symbolic acts of investigating the issue, the administration showed a stronger stance when the scandal pertained to Chancellor Merkel herself. The tapping of her phone—even though not significantly adding to the scope of NSA spying—reinforced and intensified the symbolic image of Germany as a subject of security. While public

concern about Germany's involvement in cyber surveillance showed its aversion to Germany as a major actor in international security, Merkel's outrage over the image of a subject of security solidified a contradiction in priorities between public and government interest. The progression of the scandal, therefore, highlighted symbolic representations of pacifism within the German public on the one hand, and the desire of the government for more autonomy and trust in security affairs on the other.

The revelation of NSA spying in the summer of 2013 brought forth strong reactions across the entire political spectrum in Germany. As newspapers reported, Germany was the main target of the NSA, creating a rift of trust in the transatlantic relationship (DW, 2013). Taking place in the middle of political campaigns for the federal elections in September, the issue became highly politicized. Initial reactions seemed to solidify the common stance that Germany had the responsibility to investigate the issue. Some officials even suggested imposing pressure on the U.S. administration by pausing talks regarding a new transatlantic trade agreement or refusing to pass along passenger information of flights headed towards the United States (Zeit, 2013). Others pleaded for German and European support for Edward Snowden and introduced the idea of granting him asylum in Germany. They referred to the OSCE and the Council of Europe who had preexisting regulations on the support of whistleblowers (DW, Spiegel, 2013).

Despite all these reactions, Chancellor Angela Merkel seemed to avoid the topic altogether and hesitated to take a stance in the issue. Instead of confronting the Obama administration, she sent representatives to the United States to investigate the degree to which the NSA spied on German citizens, the government, and private corporations. In

mid-July, Interior Minister Hans-Peter Friedrich of the Christian Social Union (CSU) met with U.S. Vice-President Joe Biden, Attorney General Eric Holder, and chief counter-terrorism advisor Lisa Monaco. He stated that the U.S. representatives acknowledged the German need for privacy and increased transparency in the surveillance process between the two governments. To enable further cooperation, the NSA would begin a "declassification process." Additionally, Friedrich was assured that the U.S. was not engaging in economic espionage. The interior minister concluded that the NSA surveillance program is quite focused on targeting specific data on terrorist attacks, organized crime, and non-proliferation. As a response to the minister's optimistic report of his meeting, the opposition criticized his diplomatic approach. Stating that the meeting did not meet the expectation of receiving detailed information on the surveillance program, the SPD and the Greens characterized it as a mere attempt to showcase concern (DW, 2013). Friedrich's visit turned into a highly politicized event, employed by the opposition to accuse the Chancellor and her party for downplaying the scandal.

Similar accusations followed a hearing with Merkel's Chief of Staff Ronald Pofalla in front of the intelligence committee at the end of July. The committee chairman concluded that the hearing had not resulted in any progress. Statements by Pofalla rather complicated the declassification process, which other government officials demanded. According to Pofalla, the German intelligence community had not been involved in NSA spying and he assured that, with regards to cyber security, the secret service had exercised within the realm of the German legal system (DW, 2013). This statement seemed to downplay the capabilities of the German foreign intelligence service, the Bundesnachrichtendienst (BND), which is one of the few of its kind in the world that,

according to a Spiegel article in June 2013, had invested in information technology for surveillance purposes. The article suggested that greater control of Internet activities has become one of the major priorities of Gerhard Schindler, the head of the BND who announced in 2012 a plan to invest 133 million dollars in the surveillance department (Spiegel, 2013). Interior Minister Friedrich supported this plan by emphasizing the need for a presence of German authorities in cyberspace and the opportunities the Internet entails for criminals. These goals in the intelligence community demonstrated a lack of technological capacity rather than a lack of incentive: even though legally cleared to collect 20 percent of data from foreign Internet traffic, the BND supposedly had the capacity to regulate only a much smaller percentage (Spiegel, 2013).

Regardless of the extent to which the government collaborated with the NSA on its surveillance program, the existence of surveillance measures on a smaller scale through programs at the German foreign intelligence service (BND) showcase the German government's interest in or even security need for surveillance of cyberspace. The legal and technological limitations of the BND, however, indicate that Germany could not achieve sufficient regulation of the Internet by itself. Consequently, a gap existed and still exists between security needs and the measures that could possibly be enacted; a gap possibly filled by U.S. intelligence. Since revelations about Prism began, U.S. officials have released several reports regarding the number of terrorist attacks prevented through the collection of data. In a hearing in front of the House of Representatives Select Committee on Intelligence, Director of the NSA General Keith Alexander reported that the analysis of data through NSA surveillance had prevented 50

potential terrorist attacks globally since the terrorist attacks on September 11, 2001 (DW, 2013). Several of these attacks were supposedly prevented on German soil.

Individual reports also suggested cooperation on an EU-wide level: according to information gathered by the *Financial Times*, representatives of the Obama administration had lobbied for a loosening of privacy laws in Europe (FT, 2013). The lobbying efforts targeted the "anti-Fisa clause," which would have arguably restricted NSA spying on European citizens (FT). This clause, in addition to the silence of the government, raised suspicions among German citizens: according to a poll at the time, 87 percent believed that German security agencies had been aware of the NSA spying program while over three quarters also suspected that the government had been involved (SZ, 2013). What supported these suspicions was the relative silence of the Social Democratic Party of Germany (SPD) despite its leadership role in the opposition. Since the NSA program was said to date back to the time the previous administration was in place, a coalition government between the SPD and Christian Democratic Union (CDU), critics would have traced back policies to former and current SPD leaders. In fact, the SPD supported surveillance-related policies in 2005, resulting in Chancellor candidate Peer Steinbrück remaining silent about the scandal (DW, 2013).

Chancellor Merkel reiterated General Alexander's argument about the need for surveillance throughout the beginning phase of the scandal (Zeit, 2013). Her initial defense of NSA surveillance demonstrated her acknowledgment of American hegemony on the one hand, and the need to convey a functional value of American protection on the other. As debates over the legal aspects of cyber surveillance surfaced and suspicion about a possible cooperation increased, public reactions dismissed the idea of American

protection and prioritized German security interests in cyberspace—the protection of privacy. At a moment in which the scope of NSA spying was quite ambiguous, the Chancellor was more open to the idea of balancing German and American interests through a balance between security and civil liberties. Since only symbolic actions were taken and investigations of the issue delayed, the initial reaction of Ms. Merkel's administration suggested that there still exists a certain degree of acceptance of and interest in American protection.

The major policy debate regarding the scandal revolved around the appropriate balance between security and privacy. This debate took place specifically in the United States as the government had to address the specific concerns about security threats and their implications for privacy in cyberspace. For Chancellor Merkel, however, the contradiction in policy interests also pertained to domestic affairs, the upcoming federal election, and Germany's relationship with the United States. While President Obama's administration faced the task of balancing security and privacy, Merkel's initial obstacle was the balance between maintaining the transatlantic relationship and satisfying the public's expectation of a strong German stance in the issue. At the beginning of the scandal, she remained in the background of negotiating this balance. Having acknowledged the need for privacy, she emphasized transatlantic cooperation in cyber surveillance for the security of German citizens. In an interview with *Die Zeit*, she defended the idea of cyber surveillance, stressing that the regulation and security of cyberspace are parallel concepts. The balance between security and privacy should be an ongoing debate, as technological capacities and the security needs of the state constantly change. In this context, it would be inescapable that the intelligence services of different

governments collaborate to exchange information. Her major point behind backing security measures in the Internet was her reminder that the United States has been Germany's closest ally, and that German unification had come along with a relationship of trust and cooperation in security affairs (Zeit, 2013). She rejected parallels of the NSA with the East German Stasi, stressing that such comparisons understated the severity of Stasi operations (Zeit, 2013).

Interior Minister Friedrich took a similar stance on the topic: in an interview with *Spiegel* leading up to his visit to Washington, he assured the public of his plans to voice the privacy concerns but highlighted that anti-American sentiments were "unfair" due to the lack of information on the NSA operations (Spiegel, 2013). His approach to the meeting relied on his trust in the transatlantic partnership as he expected an open conversation "among friends;" referring to a long-standing cooperative relationship that would have to prove itself in the coming weeks and months (Spiegel). He rather avoided the question on NSA spying in EU affiliated institutions and redirected the focus towards the lack of evidence and significance of cooperation between the United States and Germany. Both Merkel and Friedrich, therefore, maintained quite passive and reconciling voices as media coverage, criticism from the opposition, and public outrage unfolded throughout the weeks.

Their statements also reflect the historical component and how pre-existing perceptions of German autonomy vis-à-vis the United States were projected onto cyber security. The symbolism of the transatlantic relationship and the upcoming 50th anniversary celebration of President Kennedy's Berlin speech provided an incentive for neutrality and patience. By rejecting comparisons between the NSA and the Stasi and by

reinforcing the value of German-American relations not only in security affairs but also in the evolution of German sovereignty, Merkel drew attention to a part of German history that seems to polarize public opinion. Table 1 shows the results of a poll by the German Marshall Fund following the scandal. The survey seeks to capture European and American views on future cooperation or independence in security affairs (Stelzenmüller; Raicher, 2013). 44 percent of Germans surveyed believed that Germany should distance itself from the United States and take a more independent approach to security policy. While only 15 percent answered in favor of closer collaboration, a third of the surveyed stated the balance between independence and collaboration should remain about the same. This outcome shows the polarization of opinions on U.S. foreign policy in Germany, which is supported by the fact that only 7 percent abstained from deciding among these three options.

Table 1: Should EU/US partnership in security/diplomacy become closer, remain about the same or should the EU/US take a more independent approach from the US/EU?

	Countries				
	GB	**France**	**Germany**	**USA**	**Sweden**
Unweighted	1047	1051	1056	1054	1017
Weighted	1047	1051	1056	1054	1017
Become Closer	134	282	159	253	234
	13%	27%	15%	24%	23%
Remain about the same	370	242	355	294	264
	35%	23%	34%	28%	26%
Take a more independent approach	275	348	464	239	321
	26%	33%	44%	23%	32%
Don't know	268	179	78	268	198
	26%	17%	7%	25%	19%

Adopted from Stelzenmüller/Raicher, GMF (2013)

The polarization also reflects Germany's unique position within the European Union. A stronger tendency towards a more independent approach implies a desire for more

autonomy and the incentive to use the new security realm of cyberspace to exercise more power and dissolve the current power structures in transatlantic relations.

The mechanism of European integration, however, revealed the limitations of Germany's scope of action. As public opinion showed the willingness for more autonomy, Chancellor Merkel's pleading for international cooperation and shifting of the debate onto the European level demonstrates the state's dependence on the European Union to achieve its security objectives (SZ, 2013). As the scandal had revolved around the contentious German-American relationship, Merkel managed to overcome this pressure by charging the European Union with more responsibility regarding data protection. This strategic shift represented an opportunity to demonstrate German leadership in Europe on the one hand, and the interrelatedness between German-American and European-American relations on the other. At the same time, the shift towards the European Union confirms that European integration serves as a counterbalance to American hegemony. Even though Germany is seeking a more active role in transatlantic security, this role seems to require the legitimization through working within the boundaries of European institutions. Accordingly, Chancellor Merkel's administration refused to take on an exceptional role in the scandal by, for instance, inviting Snowden to testify on NSA surveillance. This hesitation contradicts the exceptional role Germany played as the major target of the surveillance program, which would have legitimized a more active investigation.

Revelations of the tapping of Angela Merkel's private and official cell phones released in October 2013, despite the ambiguity of the sources at the time, dramatically ceased the German government's reconciliation efforts. Having reinforced the need for

surveillance for security purposes during President Obama's visit, Chancellor Merkel and other officials openly voiced their doubt in the current state of the transatlantic relationship (NYT, 2013). While Ms. Merkel had previously joked about not being aware of being the victim of spying herself, she now confronted the U.S. President regarding the allegations just a few months later. Her sudden shift in responding to the scandal and taking initiative resulted in criticism from the German public and her opposition; a minor challenge that emerged after her successful reelection as Chancellor. The change in tone also raised the question why Ms. Merkel chose to react specifically at this point. Critics argued that the unlawfulness of NSA spying had been proven months before, when the media first revealed the content of Edward Snowden's documents.

The shift in Ms. Merkel's stance originated from the symbolic value the new revelations held to Germany's autonomy as an actor in international security. The investment in surveillance programs through the BND demonstrated Germany's acknowledgment of security threats in the Internet. Since the BND lacked the technological capacity of implementing a sufficient regulatory cyber security program, it also acknowledged the need for collaboration with the United States. While the BND or the government might not have been aware of the scope of the NSA surveillance programs, it must have cooperated on the implementation of its own program. Chancellor Merkel remained in the background throughout the beginning of the scandal. Despite reassuring the German public of the need for privacy, she laid more emphasis on the value of cyber security. With this inactivity, she actively risked her domestic support in a critical time during her electoral campaign to restore public trust in the transatlantic relationship. She took the risk with the assumption that Germany and the United States

had equally strong participation and a mutual dependence in ensuring the security of cyberspace. The revelation of her victimization, however, removed this equal playing field on which security measures were enforced. The NSA spying programs went beyond the exchange of relevant data and revealed their sole foundation on U.S. security interests. The threat of economic espionage on German corporations intensified this perspective.

The scandal and its politicization, therefore, uncovered several issues of contention pertaining to cyber surveillance. The protection of privacy and the enforcement of security measures have traditionally been at the forefront of policy debates pertaining to security in the Internet. Especially reactions from the German public—the priority of pacifism and aversion to military involvement in cyberspace—have demonstrated that the balance between privacy and security will remain a major challenge. The symbolic aspect of and diplomatic responses to the scandal, however, have revealed the need to reorganize the roles of individual governments in enforcing this balance. The scope of the NSA programs has shown that autonomy in cyber security—the ability to enforce one's own security needs and views regarding privacy in cyberspace—is determined through technological capacity. Chancellor Merkel's shift in reacting more dominantly consequently represents the acknowledgment of the Internet as a valuable resource in the security realm on the one hand, and the need for an equal playing field in utilizing this resource as a security measure on the other.

Virtual Fear and Cyber Surveillance

The scandal brought forth the inevitable need for a more equal playing ground in utilizing cyberspace as a resource for international security. The creation of this equal playing ground requires an evaluation of the various security threats. Current evaluations, however, mainly rely on speculation and a continuation of broader security strategies in the realm of cyber security. Different policy responses reflect the priorities, values, and security needs states ascribe to cyberspace and complicate the equal utilization of the Internet as a security resource. A look at the legal and institutional structures pertaining to cyber security and privacy reveal a strong divide in security objectives between the United States and Europe. Even before the September 11 attacks, the Foreign Intelligence Service Act (FISA) built the foundation for prioritizing the security of cyberspace through regulation and surveillance over the protection of privacy. Subsequent changes in the administration of intelligence services, along with more drastic legal changes after 9/11 amplified the exaggeration of security and intelligence in cyberspace. These events have demonstrated the intensifying of an environment of fear and the value of gathering data in the United States. In contrast, states in continental Europe, particularly Germany, have—based on an evaluation of their legal systems—viewed the protection of privacy in cyberspace as a security objective in itself. While possible collaboration with NSA surveillance and the implementation of similar programs in Germany may indicate an interest in cyber surveillance, the relationship between intelligence and privacy is by far less out of balance as it is in the United States. The analysis of legal systems and institutions provides an understanding of how individual states and their intelligence services attempt to enforce their security objectives in a space that lacks international

regulation. This understanding contributes to the overarching discussion on state sovereignty in cyber security.

Cyber surveillance represents one of the many policy responses to cyber terrorism and is the strategy for which the NSA has drawn public and international criticism in the last year. James Gravelle notes that intelligence agencies have dramatically increased their surveillance in recent years—a result of the fact that terrorists have quickly adapted to the information revolution, now potentially having the capacity to employ more advanced technology to disrupt the security of states (Gravelle, 111). As Gravelle puts surveillance in the broader context of knowledge-management, he points out that this process consists of several steps, ranging from the gathering of data to evaluation, interpretation, and to information exchange with other organizations (113, 119). Even though governments can extract useful information from data through the management of knowledge and close evaluation of data, he notes that, "many organisations simply store rather than process data. This mindset often over-focuses on the quantitative approach, concerned with capturing figures and numbers. The second stage in the process is to transform data into information" (113). Gravelle's findings suggest that intelligence services generally do not implement efficient programs to target specific information on terrorist activity but are rather driven by an irrational exaggeration of security threats and desire for perceived protection in the short-term.

The excessive focus on the quantity of data gathered reinforces the psychological effects of speculative nature of cyber terrorism. Thomas suggests that online propaganda and the wide variety of outlets for public messages allow terrorist groups to exaggerate their scope of influence and actual size (Thomas, 115). This strategy, according to

Thomas, "produces an atmosphere of virtual fear or virtual life. People are afraid of things that are invisible and things they don't understand" (115). Statements by Theresa May, the British Home Secretary, from 2011 confirm Thomas's argument: upon warning against the growing sophistication of the technological knowledge of terrorist groups, May specifically referred to al Qaeda, a group that supposedly called for "cyber-jihad" (Awan, 21). For British and U.S. officials, possible vulnerabilities in cyber space and the exaggeration of terrorists' online presence have created an environment of fear that has resulted in the transformation of cyber surveillance into a top priority in national security.

As Gravelle's theory implies, this priority has manifested itself in the way in which U.S. and British intelligence agencies conduct cyber surveillance. It has also manifested itself in several institutional and policy changes that facilitate the implementation of cyber surveillance and other security measures. The U.S. Air Force, for instance, included cyberspace in its mission statement as one of its domains of protection and established the Air Force Cyber Space Command in 2005 and 2006 respectively (Joyner, 2012, 163-64). Additionally, the United States Cyber Command—lead by General Keith Alexander—was added to the Defense Department in 2010, furthering the militarization of the Internet (164). Jason Healey argues that the classification process initiated by General Alexander marked the beginning of an imbalance between security and privacy in the United States; enabling the NSA to enforce its security values onto cyberspace without government regulation: "Since classification levels permitted few, if any, outside voices, the seeming consensus helped convince U.S. policymakers to adopt General Alexander's 'collect it all' strategy and create a new U.S. Cyber Command to streamline military cyber power" (Healey, 2013).

The NSA case has demonstrated how classification and few institutional changes can contribute to the militarization of cyberspace. The environment of uncertainty and semi-imaginary understanding of a perceived security threat in cyberspace to which Patrick Jagoda (2012) refers to as "Speculative Security" have legitimized excessive data gathering by U.S. and British intelligence services. The governance of the NSA by General Alexander has also confirmed Gravelle's and Tim Read's observation that domestic and international cooperation among different institutions is crucial to managing information and that the isolation of a particular organization can undermine sovereignty and limit the efficiency of security measures (Gravelle, 119; Read, 2012, 159).

Data Protection in the United States and Germany

While the perceived threat originates from speculation, the security measures have severe implications for the protection of privacy. The Foreign Intelligence Service Act of 1978 and subsequent amendments perfectly exemplify these implications. FISA represented an exceptional rule to criminal investigations: traditionally, the Fourth Amendment protected U.S. citizens from unwarranted searches without probable cause. FISA lowered the standards by which intelligence services were able to receive warrants; a measure legitimized by the significance of foreign intelligence investigations (Jaeger, Bertot, McClure, 2003, 297). Since put in place until the year 1999, the Foreign Intelligence Service Court (FISC), overseeing the investigations under FISA, received 11,883 FISA warrants—all of them were granted (Jaeger et al., 297). Adding to the already wide range of actions FISA granted intelligence services, the September 11

attacks in 2001 brought forth the passing of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("Patriot Act"), which, according to Jaeger et al, increased this range of action (299-300). The following table shows the ways in which the Patriot Act was expected to alter selected regulations of the Foreign Intelligence Service Act:

Patriot Act (Section of Act)	**Proposed Patriot II (Section of Draft)**
Intelligence need only be a "significant" purpose of an investigation (§ 218)	Expanded definitions of "foreign powers" (§§ 101-102, 111)
Records now include any tangible thing that could contain information (§ 215)	Subject of investigation need not be violating federal law (§ 102)
The secrecy clause prevents discussion of investigations (§ 215)	Immunity for private entities that voluntary provide information (§ 313)
Expanded use of roving wiretaps, pen registers, and trap and trace devices (§§ 206-207, 214, 216)	Simplified access for investigators to credit and financial information (§ 313)
Surveillance of electronic and voice mail communications (§§ 209-210)	Increased Attorney General powers to authorize warrantless FISA investigations (§§ 103-104)
Increased sharing of information from investigations between agencies and levels of government (§ 203)	Prohibition against the use of encryption technologies (§ 404)
	Further expansion of information sharing from investigation between government agencies (§ 105)

Table adopted from Jaeger et al., 2003, 299

While these laws have expanded the legal ground for intelligence services to conduct surveillance, they lack the counterbalance of institutions or laws protecting the privacy of all U.S. citizens. The Fourth Amendment, which confines the protection of privacy to preventing home searches without probable cause, has built the constitutional foundation for data protection in the United States. Since its framing is largely limited by the physical space of the home, however; it has often been at the center of debate since the United States has increasingly relied on information technology since the 1920s

(Harper, 2006, 33). The Privacy Act of 1974 marked an adaptation to the privacy needs of citizens in the information age, pertaining mostly to the maintaining of records and a requirement for agencies to disclose purposes and means of record keeping (38). However, the U.S. Justice Department, in an evaluation of the Privacy Act in 2004, noted that its broad and ambiguous regulations complicate its application, making it rather useless in adequately ensuring privacy (38). Harper notes that intelligence services still maintain some freedom to overcome the citizen's rights based on the lack of clarity in the disclosure process: "Privacy Act statements, which are required on the forms used to collect information from citizens, are insufficient in that they do not remind citizens that uses of information can be changed merely on notice published in an obscure publication called the Federal Register" (38). He adds that the influence of the U.S. Privacy Protection Study Commission, which took charge of evaluating and reporting on the efficiency of the Privacy Act in 1975, lasted for only two years when it released "Personal Privacy in an Information Society" in 1977 (38). More recent legal adaptations that responded especially to the rise of businesses in cyberspace mostly pertained to very specific groups of individuals operating online (42). These include, among others, the oversight of privacy practices for children, individuals and organizations in the health care sector, and firms in the financial services industry (40-41).

In addition to the legal measures regarding privacy in the United States, the assignment of institutions that oversee privacy protection reveals a more economically minded approach to privacy: as only few states such as California have established freestanding institutions specifically overseeing privacy concerns of citizens, the Federal Trade Commission (FTC) serves as the main regulator of consumer privacy (47). Axel

Spies argues that, while the FTC deals with cases of privacy concerns in cyberspace, it is mainly concerned with the broader concept of consumer protection (Spies, 2012, 10). This fact exemplifies the key difference between German and U.S. perceptions of privacy: in Germany, privacy implies the legal obligation of data protection; in the United States, privacy refers to a right to privacy, which falls under the broader range of rights citizens are granted as consumers (8).

The analysis of the legal developments regarding surveillance and privacy confirm the way in which pre-existing ways of law enforcement and exercise of power translate onto the governance of cyberspace. Even though U.S. Congress implemented the Privacy Act and subsequent specialized laws on areas in cyber security, it did not adequately adapt its laws to the increasing need of privacy in cyberspace to limit the scope of exercising sovereignty. Instead, the combination of FISA and Patriot Act reinforce the priority on intelligence. The United States not only maintained its pre-existing security measures but also extended them to fully utilize the wealth of information cyberspace generates.

5. Conclusion

Cyberspace has revealed itself as a new territory in which states seek to follow their security objectives and, in broader terms, to enforce their sovereignty. Even though distinct features of cyberspace—the present lack of legitimization of sovereignty, the ambiguity of territory, and the accessibility of private information—require a drastic redefinition of how sovereignty manifests itself, states still resort to traditional measures of exercising power. In the case of German-American relations, the United States seeks

to project its longstanding hegemony and its past influence on German sovereignty onto its security measures in the cyber realm. Germany's reemergence in international security, however, has decreased the functionality of U.S. influence in German security, causing the state to desire a more active role in enforcing its security values. Due to the evolution of German sovereignty, however, this more active role can exist merely within the context of EU integration and security policy. This polarization between U.S. and European security interests has traditionally presented a short-term issue in transatlantic relations; the manifestation of these differences in cyberspace, however, creates a long-term governance issue.

While the United States could rely on short-term coalition building with regards to conflicts in Iraq and Afghanistan, for instance, the significance of cyberspace in redefining state sovereignty creates a more fundamental issue that requires a collaborative evaluation of security threats and an equal playing ground to react to these threats. International cooperation would help eliminate the speculative nature of cyber security and eventually the exaggeration of security measures. Additionally, it would build the foundation for international norms in protecting privacy and combating cyber crime and future threats of cyber terrorism. Increased transparency among states, particularly in the transatlantic partnership, would benefit not only the protection of civil liberties but also the effectiveness of intelligence services in cyberspace. As Gravelle's study has demonstrated the ineffectiveness of present cyber surveillance programs due to a lack of information production, more transparency and information exchange would allow intelligence services across the Atlantic to target and evaluate information in a more focused, qualitative manner. Since German officials have acknowledged the need

for a certain degree of surveillance in cyberspace, the realization of this cooperative approach depends on the United States' acknowledgment of the new power dynamic within the transatlantic community and a more proactive oversight of its intelligence service in cyberspace.

This dependence indicates that, at this point, German foreign policy in the cyber age remains linked to U.S. foreign policy interests. The link represents a historical remainder of Germany's unique reemergence as a sovereign and autonomous actor in international security. Therefore, the development of cyberspace provides an occasion to redefine not only state sovereignty but also the underlying values and interests shaping the future of German-American relations.

Acknowledgments

I am grateful for the support I have received from the Honor Scholar Program throughout my four years at DePauw University. I particularly thank Dr. Kevin Moore for challenging me to explore new ideas and Amy Welch for supporting me throughout the thesis process. I owe special thanks to my thesis committee—Dr. Deepa Prakash, Dr. Smita Rahman, and Dr. Inge Aures—for helping me explore my intellectual interest and developing this thesis.

Work Cited

Adams, James. “Virtual Defense.” *Foreign Affairs* (2001), 80.3.98-112. Web.

Amman, Melanie; Becker, Sven; Feldenkirchen, Markus; Gude, Hubert; Schindler, Jörg; Stark, Holger; Wiegrefe, Klaus. “The German Prism: Berlin Wants to Spy Too.” *Spiegel Online* (June 2013). Web.

Andres, Richard B. “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence.” *Cyberspace and National Security*. Ed. Derek S. Reveron. Washington: Georgetown UP, 2012. Print.

Andrews, David. “The United States and its Atlantic partners.” *The Atlantic Alliance Under Stress*. Ed. David Andrews. New York: Cambridge UP, 2005. 56-80. Print.

“Asyl für Snowden: ‘Welcome Edward!’” *Spiegel Online* (November 2013). Web.

"Aufklärung außer Rand und Band." *Zeit Online* (October 2013). Web.

Awan, Imran; Blakemore, Brian. *Policing Cyber Hate, Cyber Threats and Cyber Terrorism.* Burlington: Ashgate Publishing Limited, 2012, Print.

Awan, Imran. “Cyber Threats and Cyber Terrorism: The Internet as a tool for Extremism.” *Policing Cyber Hate, Cyber Threats and Cyber Terrorism.* Ed. Imran Awan; Brian Blakemore. Burlington: Ashgate Publishing Limited, 2012, Print.

Blakemore, Brian. “Cyberspace, Cyber Crime and Cyber Terrorism.” *Policing Cyber Hate, Cyber Threats and Cyber Terrorism.* Ed. Imran Awan; Brian Blakemore. Burlington: Ashgate Publishing Limited, 2012, Print.

Conway, Maura. “Terrorist ‘Use’ of the Internet and Fighting Back.” *Oxford Internet Institute* (September 2005). Web.

Denning, Dorothy E. “Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.” *The Terrorism Research Center* (05.23.2000). Web.

Dettke, Dieter. *Germany Says “No.”* Baltimore: Johns Hopkins UP, 2009. Print.

Dick, Wolfgang. “Pressure on Merkel to talk 'Prism' with Obama.” Ed. Michael Lawton. Deutsche Welle (June 2013). Web.

Farrell, Henry; Finnemore, Martha. “The End of Hypocrisy.” *Foreign Affairs* (November/December 2013). Web.

Fontanella-Khan, James. "Washington pushed EU to dilute data protection." *Financial Times* (June 2013). Web.

Goldman, David. "Hacker hits on U.S. power and nuclear targets spiked in 2012." *CNN Money* (2013). Web.

Goldman, David. "Nations prepare for cyber war." *CNN Money* (2013). Web.

Gravelle, James. "Knowledge Management and Cyber Terrorism." *Policing CyberHate, Cyber Threats and Cyber Terrorism.* Ed. Imran Awan; Brian Blakemore. Burlington: Ashgate Publishing Limited, 2012, Print.

Haftendorn, Helga. *Coming of Age. German Foreign Policy Since 1945*. Munich: Rowman & Littlefield Publishers, Inc, 2006. Print.

Harper, Jim; Spies, Axel. "A Reasonable Expectation of Privacy? Data Protection in the United States and Germany." *AICGS Policy Report* (2006). Web.

Healey, Jason. "How Emperor Alexander Militarized American Cyberspace." *Foreign Policy* (November 2013). Web.

Jaeger, Paul T.; Bertot, John Carlo; McClure, Charles R. "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act." *Government Information Quarterly* 20 (2003). 295-314. Web.

Jagoda, Patrick. "Speculative Security." *Cyberspace and National Security*. Ed. Derek S. Reveron. Washington: Georgetown UP, 2012. Print.

Joyner, James. "Competing Transatlantic Visions of Cybersecurity." *Cyberspace and National Security*. Ed. Derek S. Reveron. Washington: Georgetown UP, 2012. Print.

Markovits, Andrei; Reich, Simon. *The German Predicament. Memory and Power in the New Europe.* Ithaca: Cornell UP, 1997. Print.

Medick Veit. "Innenminister im Interview: Friedrich beklagt mangelnde Fairness gegenüber den USA." *Spiegel Online* (July 2013). Web.

"Merkel plädiert für internationales Datenschutzabkommen." *Süddeutsche Zeitung* (July 2013). Web.

"Merkel's top aide plays down allegations of bulk US spying on Germans." *Deutsche Welle* (July 2013). Web.

"Merkel verteidigt Abhören von Telefonaten" *Zeit Online* (July 2013). Web.

"NSA claims surveillance program foiled 50 terror plots" *Deutsche Welle* (June, 2013). Web.

Nye, Joseph. "The Information Revolution and the Paradox of American Power." *American Society of International Law*. Vol. 97 (April 2003). Pg 67-75. Web.

Reveron, Derek S. *Cyberspace and National Security*. Washington: Georgetown UP, 2012. Print.

Seeney, Helen. "'The EU should grant Snowden the right to stay.'" Ed. Michael Lawton. *Deutsche Welle* (July, 2013). Web.

Smale, Alison. "Anger Growing Among Allies on U.S. Spying." *New York Times* (October 2013). Web.

"SPD, Greens slam Interior Minister Friedrich after US surveillance talks in Washington." *Deutsche Welle* (July 2013). Web.

Spies, Axel. "Personenbezogene Daten aus Internationaler Perspektive." Presentation in Berlin: Bingham, 2012. Web.

Stelzenmüller, Constanze; Raicher, Josh. "Transatlantic Majorities Oppose Domestic Surveillance." *Issue Poll 2013: Surveillance*. GMFUS (2013). Web.

Stohl, Michael. "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?" Crime, Law and Social Change. Springer Science (2007). Web.

Tewes, Henning. *Germany, Civilian Power and the New Europe.* New York: Palgrave, 2002. Print.

"The Unadventurous Eagle; German Foreign Policy." *The Economist* (May 2011). Web.

Thomas, Timothy L. "Al Qaeda and the Internet. The Danger of 'Cyberplanning.'" *Strategic Studies Institute* (2003). Web.

Trachtenberg, Marc. "The Iraq crisis and the future of the Western alliance." *The Atlantic Alliance Under Stress*. Ed. David Andrews. New York: Cambridge UP, 2005. 201-231. Print.

"Vize-Präsident Biden überrascht Friedrich." *Deutsche Welle* (July 2013). Web.

Wittlinger, Ruth. "The Dynamics of Collective Memory and German Foreign Policy Since Unification." *AICGS Policy Report* (2013). Vol. 57. Web.

Zimmermann, Hubert. “Security exporters: Germany, the United States, and transatlantic cooperation.” *The Atlantic Alliance Under Stress*. Ed. David Andrews. New York: Cambridge UP, 2005. 152-176. Print.