International Journal of Information Science and Management
Vol. 24, No. 1, 2026, 199-226
DOI: https://doi.org/10.22034/ijism.2026.2022560.1395 / DOR: https://dor.isc.ac/dor/20.1001.1.20088302.2026.24.1.10.1

Original Research

Techno-geopolitics and the Sociopolitical Aspect of Information Science: A Case Study of the US Cyber Strategy in the Obama Administration

Farnaz Noori
Assistant Prof., Department of Transregional and Global Studies,
University of Tehran, Tehran, Iran.
farnaznoori@ut.ac.ir
ORCID iD: https://orci.org/0000-0002-1414-7703

Received: 09 February 2024
Reviewed: 18 February 2024
Accepted: 02 September 2025

Abstract

The study of Sociological aspects of information science, as the interplay of science and social structures, gained academic attention and popularity throughout the 1980s. Today, cyberspace, as a primary domain for information creation, dissemination, and consumption, is the subject of extensive sociopolitical research and analysis. Meanwhile, Cybersecurity is an emerging component of national security and continues to play a more crucial role in international relations. A vast body of literature has emerged on how politics and international relations are influenced by the emergence of cyberspace. This literature regards cybersecurity as a dimension of national security and considers its role in international relations. This article examines the relationship among cyberspace, national security, and geopolitics. It focuses on the United States of America as a cyber power to examine how cyber issues have been linked to the national security agenda and have informed decision-making in the country in the 21st century. This renders the entire work a case study and sheds light on the American approach to addressing the cyber threat in the Information Age. Relying on an extended version of the Copenhagen School and its theory of securitization, and using process-tracing as the research method, the author argues that, as an instance of the interaction between technology and geopolitics, the US cyber strategy in the Obama Administration involved a securitization process aimed at stabilizing America's informational superiority. The process is then analyzed within a framework of the country's security priorities and information policy in the 21st century.

Keywords: Techno-Geopolitics, Securitization, The US Cyber Strategy, Information Technology, National Security, Information Science, Sociopolitical Aspect.

Introduction

The rise of information technology revolutionized data storage and use and marked a turning point in nearly all aspects of social life. Historical evidence abounds over the socio-political impact of technological achievements (Butler, 2001). Radio, cinema, and mass media transformed modern societies in the mid-20th century just as steam power and factories changed

industry in the 1700s (Deutsch 1957, in Cavelty, 2007, p. 13) and Fordist technologies impacted forms of social relations in Russia/the Soviet Union (Bailes, 1981; Gerschenkron, 1962; Trotsky, 2009, all in McCarthy, 2013, p. 471). Likewise, the information revolution is regarded as "the third industrial revolution" (Nye Jr, 2010, p. 1; Rifkin, 2011), with profound impacts on the economy, culture, and politics. When considered within national security, cybersecurity must be addressed from the perspective of security studies, as articulated by experts in foreign policy and international relations. From their viewpoint, the complex challenges of the 21st century are manageable only if "*a cyber-inclusive view of international relations"* (Choukri, 2015, p. 11) is developed. Just as developments in cyber technology change cybersecurity preservation mechanisms, the way *security* is conceptualized within security studies determines how cybersecurity and national security are linked. In this sense, cybersecurity is an *evolving interdisciplinary concept,* reflecting the latest developments in Information Technology and informing conceptualizations of Security Studies curricula.

In this research, the author investigates how the interaction between technology and geopolitics affected the U.S. cyber strategy during the Obama Administration. The argument is that the US cyber strategy in the Obama administration involved an 'informational superiority stabilization' process in the form of 'gathering as much information as possible by global mass surveillance on Internet users', explicable as an act of securitization. Espionage and state surveillance are integral to the intelligence communities of any country seeking to access information about the decision-making of foreign states. It automatically involves the use of human sources to obtain information of interest through wiretapping of cell phones, satellite imagery, and other means, to gain greater knowledge of other states' capabilities or intentions (Deeks, 2015, p. 298). Banks (2017, p. 513) defines cyber espionage as "deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks".

Technologically, cyber intelligence involves the use of "systems dealing with communications data (surveillance systems monitoring phone calls, emails, Internet activity, etc)" (Cayford & Pieters, 2018, p. 90). In this article, the author argues that, alongside the development of new technologies, the Obama administration pursued a strategy of informational superiority stabilization through mass surveillance and systematic cyberespionage against US citizens and worldwide to preserve US national security and geopolitical interests. This is where the concept of 'technogeopoltics is involved. Butler's (2001) idea of 'techno-geopolitics' in '*Technogeopolitics and the Struggle for Control of World Air Routes*', published in 2001, looks pertinent to the subject. He describes the concept as a lens for analysis, which clarifies "the recursive relationship between technology and geopolitics". According to Butler, technological achievements can affect political, mostly diplomatic, positions of states, and this clarifies a relationship between technology and geopolitics. Although Butler does not claim that his conceptualization is applicable to all geopolitical events, he seeks to develop a framework with five themes to clarify where technology and geopolitics overlap in scope (Yannakogeorgos, 2009).

In the 1980s, the ideas of Social Construction of Technology (SCOT) and Actor-network Theory (ANT) were widely used and cited in the sociological literature on the sociological aspects of information science, particularly as accounts of the interplay between science and social structures (Gilchrist, 2009, p. 119). This manuscript contributes to the information science literature in terms of regarding 'information' as a key to national security for long-term

strategy making. Taking information policy as "an umbrella term for all laws, regulations, and doctrinal positions that deal with information, communication, and culture" (Braman, 2011, p. 2), this article provides insight into how the US official decisions on the ways for information processing, access, and use have been shaped by the country's strategic needs. As policy making in information sciences usually involves establishing guidelines and regulations that govern how information is stored, provided,d and used in society, the US national security strategies in the post 9/11 years have included drawing on mechanisms whereby information is gathered, integrated, and stored to preserve national security.

Literature Review

A typological classification of the literature on this subject should situate the US cyber strategy within the broader framework of discussions in geopolitics and international relations. A good thematic basis exists in literature, which makes it possible to clarify how drawing a link between geopolitics and technological developments creates a central question based on which the whole literature on this subject can be categorized: is it technology that impacts politics and creates changes in the international system, or it is it politics that impacts technological achievements? In International Relations, two distinct approaches, rooted in the philosophy of science, can be traced regarding the impact weight and direction of the interaction between geopolitics and technology. As far as the subject of this article is concerned, the two approaches create grounds for categorization of related literature based on the interaction of technology and geopolitics (Figure 1) and lets for the main research question to arise: How is the interaction between technology and geopolitics embodied in the US cyber strategy in the 21st century?

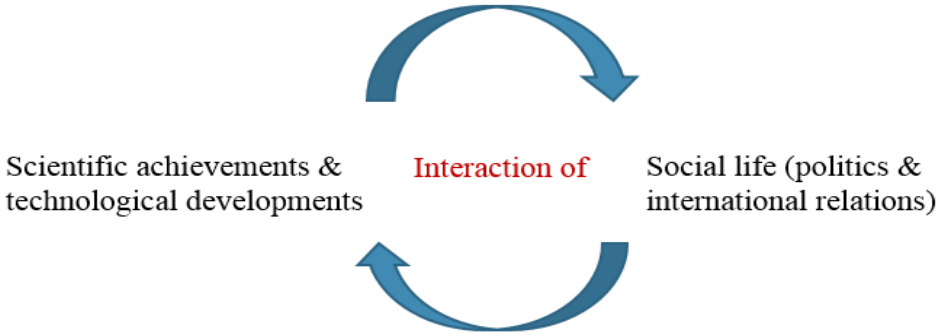

Figure 1: Conceptual basis for categorization of literature on the relationship between information technology and international relations

Drawing substantial emphasis on the impact of technological achievements on politics and international relations underpins technological determinism, which holds that technological developments determine how social structures change. Indeed, socio-political changes are bound to move in the direction technological achievements determine. According to determinists, social development is an outcome of the linear rationality of technological developments (McCarthy, 2013, p. 473). McCarthy (2013, p. 473) highlights four elements of this definition: an absence of human agency, a teleological element in the form of a linear process for technological development, a realist ontology, and a causal argument for the social outcome of technological development.

McCarthy (2013, p. 473) distinguishes between two types of technologically determinist

arguments: technological instrumentalism and technological essentialism. The instrumentalist view regards technology as neutral and as an instrument of human action. According to this strand of determinism, no technological achievement necessarily yields a specific outcome. Neither do nuclear weapons change the structure of international politics, nor does the Internet lead to democracy. Technological advancements take place *in abstraction* from the social context, and this context does not affect their findings. Essentialists, by contrast, assert that technology has an essence that shapes social and political relations. While the central argument of instrumentalists is *the neutrality of technology, essentialists believe that technology is autonomous and directs social relations toward the purposes inherent in its own objectives*. This leads many essentialists to argue "for a rejection of the technological and a return to simpler forms of life" (McCarthy, 2013, p. 475). The essentialist understanding of technological determinism relies on strains of Marxist thought, which means of production create the basis for social class.

Both strands of technological determinism regard technology as the driving force behind social change and exclude the role of human choice in technology development. According to Wyatt (2008, p. 169, in McCarthy, 2013, p. 476), a problem with technological determinism is that "it leaves no space for human choice or intervention and, moreover, absolves us from responsibility for the technologies we make and use". In International Relations, McCarthy (2013, p. 476) points to the neglect of the concept of power as the central driving force in world politics, as a result of a deterministic view of technology. Inspired by a pre-Kuhnian conception of the cumulative nature of scientific knowledge, determinists regard technology as the driving force behind social change and exclude the role of human choice in its development. The logic of technological determinism has led many to view the Information Revolution as the cause of substantial changes in international politics. As Cavelty (2007, p. 12) puts it, the fact that major segments of social life, such as culture, business, entertainment, and research, are revolutionized by the new technology makes it easy to become excited about "the transformative power of new information and communication technologies". According to Cavelty (2007, p. 12), "technological determinism is and has been an alluring temptation, as a look at the past shows: the conviction that the world is about to enter into a new phase of history is a near-permanent feature of modern life, mirroring a belief in an unbroken line of constant progress closely linked to technological development".

The second spector, *technological constructivism*, is best known through the work of Geoffrey Herrera and Stefan Fritsch. In *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*, Herrera (2006) observes that technologies such as the railroad or the atom bomb have had consequences for the international system; yet, he notes that these are the *products* of the same system and do not leave a one-way impact on it. Constructivists emphasize on "the social forces that shape the emergence of technology" (Misa, 2008, p. 230) and "the central role of human agency in constructing scientific objects of study, and of the political, cultural and economic determinations of technological design" (McCarthy, 2013, pp. 470-471). Buzan and Hansen (2009, p. 54), for example, reject the idea of technological determinism, stating that the evolution of nuclear technology in the 20th century, though it affected the political process, was itself shaped by the bipolar system derived from US-Soviet confrontation. There is a "complex process of feedback" between technology and human decision-making, not one of determinism. Technological constructivism holds that major technological developments do not occur in the

abstract; they require government support, sponsorship, and budget allocation; indeed, politics determines which technologies to develop.

A third type of the related literature focuses on information policy, by defining the concept as "the proprioceptive organ of the nation-state, the means by which it senses itself and, therefore, the medium through which all other decision-making, public or private, takes place (Braman, 2006, p. 4). As far as the subject of this article is concerned, a huge literature is produced on the necessity of creating a balance between 'surveillance' on the part of nation-states as part of their information policy and citizens' privacy (Jones et al., 2020; Friedman & Hendry, 2019; Gill, 2028; Kiernan & Mueller, 2020). Some scholars have studied the status of individual rights, including privacy and governments' information policies, at the national or regional scale. Holt and Malčić (2015), for example, have compared the regulatory strategies of the European Union and the United States, and the resulting contrast between policies governing privacy in the digital space. Brier, Jr. (2017) discusses the way the limits of governmental access to personal data stored in the cloud should be defined. Focusing on the Republic of Ireland, the author analyzes the so-called "*Microsoft Ireland*" case, as a technical opportunity in the US Court of Appeals case, according to which the Government could not obtain the contents of emails stored overseas by securing a warrant under the Stored Communications Act (SCA). In another article, Clement and Obar (2016) evaluate the data privacy transparency of forty-three Internet carriers serving the Canadian public following the Snowden revelations and propose further data privacy transparency efforts in Canada and globally.

Other classifications of this literature can be based on argumentation and subject. While some authors regard cyberspace as a source of threat to (the US) national security (McCarthy et al., 2009; Choucri & Goldsmith, 2012; Dunn, 2005), others regard it as a component of national power (Kuehl, 2009; Nye Jr, 2010; Fuerth, 2009).

Theoretical and conceptual framework

Theoretically, the concept of techno-geopolitics is useful for addressing the research question when applied in conjunction with an extended version of the Copenhagen School's theory of securitization. The Copenhagen School emerged in the 1980s and was further developed in the 1990s as the most influential framework for security analysis at the time. Inspired by the English tradition in international relations, the Copenhagen School is prominent for its discussion of subject-level security and the concept of securitization.

The Copenhagen School holds that the concept of security should be extended to areas other than the military and thus defines five sectors of security: The *military sector,* the *political sector,* the *economic sector,* the *societal* or *socio-cultural sector,* and the *environmental sector* (Buzan & Little, 2000, pp. 73–74). As Emmers (2016, p. 169) states, the crucial question that arises when the definition of security is widened to include non-military issues is whether the broadening will render the concept incoherent. The Copenhagen School's contribution to the question is illustrated by the introduction of a systematic framework for security analysis grounded in the concept of *securitization*. According to Buzan et al. (1998, p. 23), issues become politicized when they require government decisions and resource allocation, and securitized when they necessitate emergency actions beyond normal political procedures. An 'act of securitization' is one that moves a concern from the politicized to the securitized domain. It is the move that deals with issues as being beyond the established rules of the game and "can

thus be seen as a more extreme version of politicization" (Buzan et al., 1998, p. 23). Taking security as a 'speech act', securitization theory is based upon a discursive conception of security and makes "the definition of security dependent on its successful construction in discourse" (Buzan & Hansen, 2009, p. 213). Indeed, security is based on a social constructivist assumption, and various elements of structural analysis are perceived in the conceptualization of security (Marandi & Halalkhor, 2016, p. 88).

Since its emergence, securitization theory has been used in security analysis and continues to be applied by many scholars, particularly in the context of immigration in Europe. But it also received criticism from inside and outside. Critiques of securitization theory target its conceptualizations of the aims and audience of securitization, as well as its "'freezing' the meaning and notion of security" (Cavelty, 2007, p. 26) within a speech-act conception. Wæver (2003, 2004 in Cavelty, p. 26) mentions the critique from the so-called 'Paris school'. Scholars from the *Institut d'Etudes Politiques de Paris* have held that the theory focuses too much on the discursive practices and ignores the *non-discursive practices* of security formation by "professionals of security" in the real world (Bigo 1998 and Aradau 2001a in Cavelty, 2007, p. 27).

In this article, to address the practical aspect of securitization, we examine the criticism that those who argue that the theory freezes the notion of security in speech acts and falls short of providing sufficient conceptualization of what extraordinary measures are. Thus, 'securitization of cyberspace' is assumed in this research to have subjective and objective aspects. The *subjective* aspect of securitization is defined as a discursive practice and is not addressed in this article. *Objective* securitization of cyberspace emphasizes the practical aspects of securitization and is not addressed by theory. Figure 2 shows subject coverage of the two aspects of securitization of cyberspace in this work. Taking securitization of cyberspace as a process with two distinct strands, this article focuses on its practical aspects. Since the author is moving beyond the theory to explain the non-discursive aspect of securitization, 'objective securitization of cyberspace' needs to be defined conceptually.

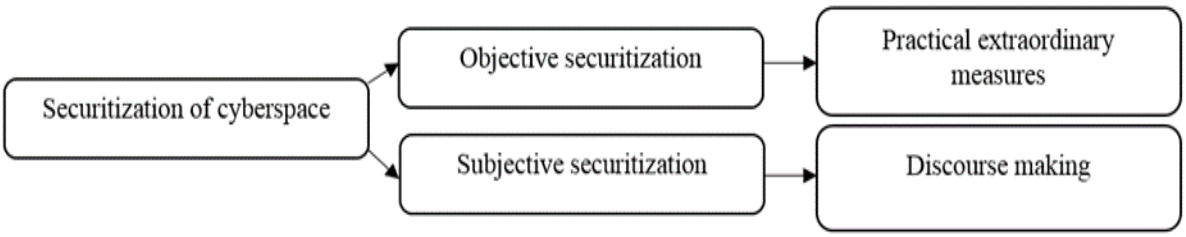

Figure 2: Basis for conceptual definition of securitization of cyberspace

An objective definition of securitization of cyberspace ought to consider an action as an act of securitization when it claims to be done for the purpose of providing cybersecurity, but is indeed 'extraordinary' and 'beyond normal political procedures' and is conducted by 'political leaders and government as the securitizing actor'. Objective securitization of cyberspace is aimed to meet basic elements of the theory and can be conceptually defined as: *Any set of coherent activities or extraordinary measures, either illegal, unconventional, and beyond normal political or legal procedures, technical and non-technical, committed by state actors with long-lasting impacts aimed to achieve security at the expense of the security or privacy of other rightful actors, such as actions that create, enhance or promote conflicts in cyberspace, extend physical world conflicts to cyberspace or increase the level of hostility and tension*

among other actors, and adopt or found strict security norms, standards and procedures conventionally used in threat situations.

Materials and Methods

The method used to answer the research question is process tracing. The method is defined as "the analysis of evidence on processes, sequences, and conjunctures of events within a case for the purposes of either developing or testing hypotheses about causal mechanisms that might causally explain the case" (Bennett & Checkel, 2012, p. 10). George and Bennett (2005, p. 206) define process tracing as the use of sources such as histories, archival documents, and interview transcripts to investigate whether and how a hypothesis derived from a theory is applicable in a given case, and to examine the sequence of events leading to a particular outcome.

The method is based on "a mechanismic understanding of causation that focuses on the process whereby causal forces are transmitted through a series of interlocking parts of a mechanism to produce an outcome" (Beach & Pederson, 2013, p. 13). It basically involves "backward from observed outcomes to potential causes—as well as forward from hypothesized causes to subsequent outcomes" (Bennett, 2010, p. 13). Process tracing is widely used in Security Studies to trace causal mechanisms in a case. Beach and Pederson (2013, pp. 11-12) distinguish three different research purposes for which process tracing may be used, and therefore explain three distinct types of process-tracing: theory-testing, theory-building, and explaining-outcome. Figure 3 summarizes the different types of process-tracing methods by research purpose.

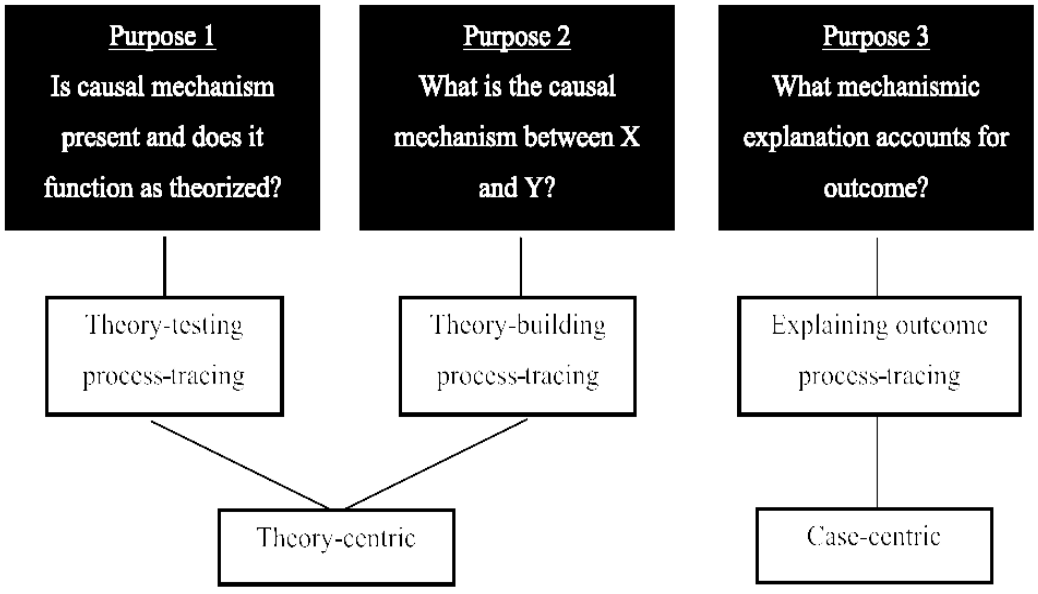

figure 3: three different uses of process tracing methods. source: Beach and Pederson, 2013, p. 12

In *the theory-testing process-tracing process, the researcher hypothesizes a causal mechanism within a case (e.g.*, X contributes to producing Y). The causal mechanism between X and Y is theoretically supported. In this model, the researcher knows both X and Y, and current theories can explain the causal mechanisms the researcher hypothesizes to exist between them.

Theory-building process-tracing is used when the researcher tries to build a theory about a

causal mechanism between X and Y "that can be generalized to a population of a given phenomenon" (Beach & Pederson, 2013, p. 11). Relying on inductive reasoning, theory-building process tracing starts with empirical observation and seeks a plausible hypothetical causal mechanism linking variables.

Explaining-outcome process tracing involves the researcher's effort to explain Y as an outcome and to explore the mechanisms that account for it. Both theory-building and theory-testing process tracing methods are "theory centric" (Beach & Pederson, 2013, p. 11), meaning that ontologically and epistemologically they fall within the "neo-positivist and critical realist positions, where the understanding is that the social world can be split into manageable parts that can be studied empirically (Jackson, 2011, in Beach & Pederson, 2013, p. 12). The researcher works to test or find generalizable theories. In these methods, the causal mechanisms are understood to be systematic factors, meaning that they can be generalized across cases that are within the context in which they are expected to operate" (Falleti & Lynch, 2009, in Beach & Pederson, 2013, p. 12). By contrast, explaining-outcome process tracing is case-centric. The researcher regards the social world as a context-specific complex where generalizations are either very difficult or impossible. Theories are used pragmatically and eclectically, "as heuristic instruments that have analytical utility in providing the best possible explanation of a given phenomenon (Peirce, 1955, in Beach & Pederson, 2013, p. 13). The objective is neither to test a theory nor is it to build one. Rather, the researcher seeks to demonstrate that a particular theory is the most explanatory for a given case. "Explanations are case- specific and cannot be detached from the particular case (Humphreys, 2010, pp. 269-270, in Beach & Pederson, 2013, p. 13). According to Jackson (2011, p. 114, in Beach & Pederson, 2013, p. 12), the ontological understanding of the world for case-centric process-tracing scholars is a "monist" one in which "the objects of scientific investigation are not inert and meaningless entities that impress themselves on our (natural or augmented) senses or on our theory- informed awareness". Explaining-outcome process tracing involves the researcher's effort to trace the causal mechanisms that lead to a specific outcome in a single case. It is not theory-centric in that, instead of trying to apply or build theories, the objective is to find the 'best explanation' for an outcome to occur. Mackie (1965, in Beach & Pederson, 2013, p. 18) elaborates on what is meant by the 'best explanation' of the outcome: "The ambition is to craft a minimally sufficient explanation of a particular outcome, with sufficiency defined as an explanation that accounts for all of the important aspects of an outcome with no redundant parts being present". Beach and Pederson (2013, p. 19) state that explaining-outcome process-tracing resembles the reasoning strategy known as 'abduction' by Peirce (1955). Yet, they recognize two parallel paths of deduction and induction within it. Figure 4 depicts how the two paths are taken together to make up the final abduction.

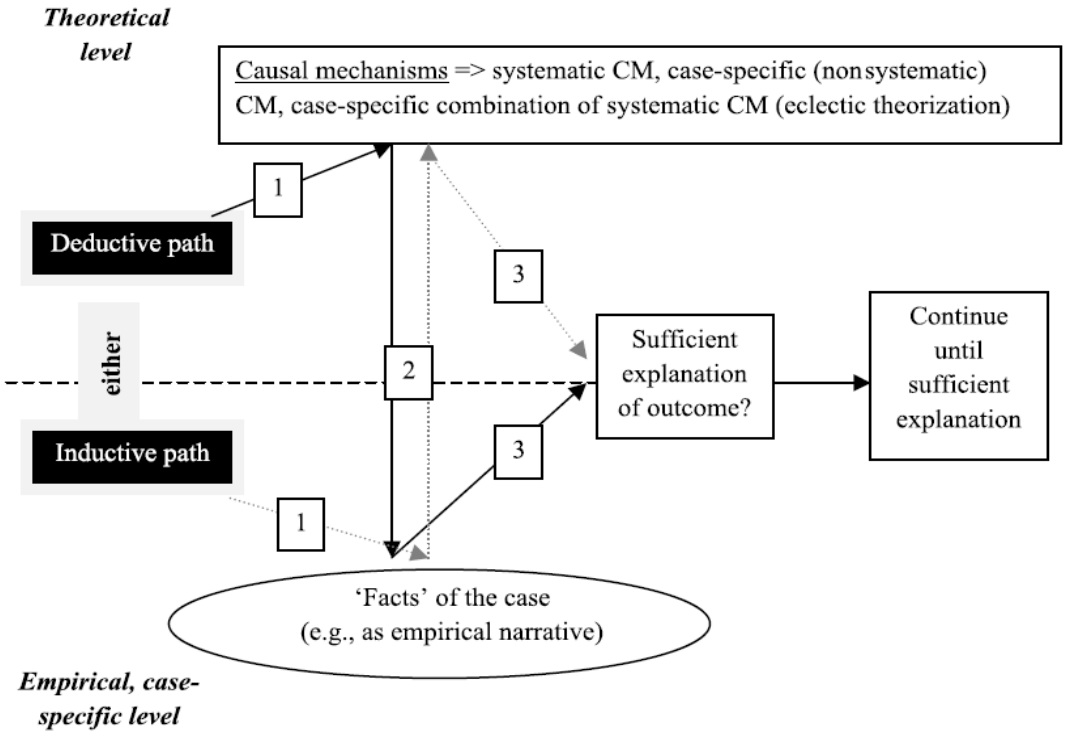

Figure 4: Explaining-outcome process-tracing. Source: Beach & Pederson, 2013, p. 20

The deductive path involves testing causal mechanisms to explain the outcome. An existing theory is conceptualized in the first step to fit the causal mechanism. Empirical tests are developed against facts of the case to test the theoretical explanation. In the final stage, the researcher assesses whether sufficient explanation is provided for the outcome. If a single deductive path is not a sufficient explanation, the research continues by repeating the deductive path, using eclectic theorization, or choosing the inductive path. The inductive path includes using empirical evidence to build an explanation. In a bottom-up approach, the researcher starts with the outcome and works backward to identify the causal mechanism that best explains it.

In this paper, the objective is to provide the best possible explanation of how objective securitization of cyberspace occurred during the Obama Administration; therefore, the explanatory process tracing method is used. What is 'traced' in this research as instances of objective securitization of cyberspace includes factual information about any initiatives taken by the US government which falls within the conceptual definition of an act of securitization in accordance with the securitizing move and beyond normal political measures such as legislation, executive orders, presidential directives, investment, recruitment, attack, contracting, intelligence, etc. Sources for data collection include firsthand production in the form of official documents, governmental regulatory publications, official reports, institutional publications of organizations, statements by chief U.S. officials in speeches, interviews, or documentaries, and information leaked by whistleblowers such as Edward Snowden. References are given to some secondary sources, including books, scholarly articles, theses, and media releases in the final analysis of the traced processes to support the author's arguments on subjects. Table 1 presents the sources of data used in the first phase.

Table 1

Sources for data collection in the first phase

NO.	Title	Production date	Publisher
1.	National Security Strategy (NSS)	2010	The White House
2.	Sustaining U.S. Global Leadership: Priorities for 21st Century Defense	2012	DoD
3.	Information Operations (JP 3-13)	2012	DoD
4.	Cyber Electromagnetic Activities (FM 3-38)	2014	DoD
5.	The US International Strategy for Cyberspace	2011	The White House
6.	Joint Cyberspace Operations (JP 3-12) document	2013	Joint Chiefs of Staff
7.	The Quadrennial Homeland Security Review	2014	DoH
8.	The White House Fact Sheet (CTIIC)	2015	The White House
9.	National Security Strategy (NSS)	2015	The White House
10.	DoD's Cyber Strategy	2015	DoD
11.	Interim National Security Strategic Guidance	2021	The White House
12.	Report to the Committee on Armed Services, House of Representatives	2019	US GAO
13.	National Security Strategy (NSS)	2017	The White House
14.	Cyberspace Policy Review	2009	Cybersecurity & Infrastructure Security Agency
15.	National Intelligence Strategy	2009	ODNI
16.	National Intelligence Strategy	2014	ODNI
17.	The US PATRIOT ACT	2001	The Congress
18.	The FISA Amendments Act	2008	The Congress
19.	Executive Order 12333	1981	The White House
20.	Cybersecurity Act of 2012	2012	The Congress
21.	The NSA website		
22.	Executive Office of the President	2012	The White House
23.	Edward Snowden interviews and leaks	2013	
24.	Presidential Memorandum on the establishment of the CTIIC	2015	The White House
25.	US-China Economic & Security Review Commission	2012	
26.	Report to the U.S.-China Economic and Security Review Commission	2012	Northrop Grumman Corporation
27.	9/11 commission report		
28.	National Security Strategy (NSS)	2002	The White House
29.	National Security Strategy (NSS)	2006	The White House

Data gathering continued until saturation was achieved, and the author found a sound idea of the way data could be 'categorized' based on the definition of objective securitization of cyberspace.

Results

The objective securitization process, as defined in the previous sections, can be traced to a specific perception of information integration. The sections below present elements of the informational superiority stabilization process in the Obama administration as stated in the

hypothesis:

Identification of information integration as a key to national security

The way 'information' is perceived by the state has implications for its long-term information policy. As a substantial requirement of the Information Age, the integration of information to dominate the strategic environment was identified as crucial to preserving national security in the US. The 2009 *Cyberspace Policy Review* (2009, p. V) stated that the government needs to have "an effective mechanism" in which information from the government and the private sector is integrated and can be relied upon for "incident response decisions". The 2009 *National Intelligence Strategy* (2009, p. 14) enumerates among its enterprise objectives the need to radically improve the application of information technology for information management, integration, and sharing both within the Intelligence Community and with other partners. The document mentions that the Intelligence Community is facing "an explosive growth in type and volume of data, along with an exponential increase in the speed and power of processing capabilities" (The National Intelligence Strategy, 2009, p. 14). Also, the 2014 *National Intelligence Strategy* (2014, p. 2) names 'cyber intelligence' among its mission objectives, and 'information sharing and safeguarding' as one of its six enterprise objectives. It recognizes the responsibility to make information available across the IC, and emphasizes having "an integrated information sharing environment" (National Intelligence Strategy, 2014, p. 13). The document maintains that information policies, processes, and systems must address these circumstances and, when integrated with information-sharing and systems, accelerate and synchronize the delivery of information and enterprise capabilities (National Intelligence Strategy, 2014, p. 14). To achieve the objectives, the IC intended to:

- Develop a world-class, Community-wide, assured information environment based on a common, effective, reliable, and secure infrastructure
- Enable the rapid implementation of simple, logical, effective, crosscutting solutions (materiel and non-materiel), recognizing the need to terminate and eliminate legacy systems.
- Integrate assured and authorized discovery and access of information to the IC workforce.
- Narrow the gap between the capacity to "sense data" and our capabilities to "make sense of data" in handling an exponentially increasing volume and variety of data and information (National Intelligence Strategy, 2014, p. 14).

Integration of information was assumed to be possible, relying on two US national assets in the Age of Information: a powerful private sector and technological superiority. The 2009 National Intelligence Strategy (2009, p. 15) mentions explosive pace in the development of technology as an opportunity to improve the IC's productivity, effectiveness, and agility, and calls for discovering and developing Science & Technology/R&D advances for the IC to overcome current and emerging adversaries. The document states that "rapid technological change and dissemination of information" provide new means for the US adversaries and competitors, but also provide the United States with "new opportunities to preserve or gain competitive advantages" (The National Intelligence Strategy, 2009, p. 4).

Adaptation, adoption, and development of technology was regarded to be gained by a combination of "technology push," "capabilities pull," and "mission pull" including the development of "major long-term collection systems to advanced analytical techniques, and clandestine sensors to secure, reliable networks and communications systems" (The National

Intelligence Strategy, 2009, p. 15). Research & Development (R&D) programs were the focus of attention for their potentials of technological innovation since they could "accelerate technology development, enhance collaboration, develop new and unexpected solutions, and protect "high risk/big payoff" projects" (The National Intelligence Strategy, 2009, p. 15)

Also, the Cyberspace Policy Review (2009, p. 18) emphasized public-private partnership as having "fostered information sharing", because it had helped the protection of critical infrastructure for over a decade. What was expected from the private sector was to play their role by sharing their data with the government: "Industry leaders can help by engaging in enterprise information sharing and account for the corporate risk and the bottom line impacts of data breaches, corporate espionage, and loss or degradation of services" (Cyberspace Policy Review, 2009, p. 17). Stating that "mission success depends on the right people getting the right information at the right time" (National Intelligence Strategy, 2014, p. 13), the IC was seeking to create databases of integrated information by sharing information both with inter-state bodies and the private sector. The 2014 National Intelligence Strategy (2014, p. 13) identifies the following to meet IC's objectives: consolidating IT requirements to build more effective infrastructure, providing the IC workforce with access to integrated information, and promoting a culture that embodies, supports, and furthers responsible information sharing. The key to achieve the goals is summarized in improving the transition of science and technology (S&T) solutions to the operational user and into major system acquisition, expanding partnerships and engagement with the academic community, industry, partner governments, mission customers, and nongovernmental centers of technical excellence and innovation, and scanning for global technology trends to find emerging and potential breakthroughs and new technology for integration into IC capabilities (Cyberspace Policy Review, 2009, pp. 15-16).

Legalization of global mass surveillance on Internet users by presidential power

A major step contributing to mass surveillance in cyberspace has been the legalization of wiretapping on US citizens and worldwide. The ground for the initiative was prepared during the George W. Bush presidency when the US PATRIOT ACT was passed in 2001, putting limitations on some civil liberties of US citizens, mainly immigrants, to guarantee national security and combat terrorism. The Act facilitated legal surveillance of U.S. citizens and immigrants by monitoring communications, financial transactions, and other activities (Lee, 2015, p. 11). Sec 202 of the Patriot Act authorizes government officials to conduct a "roving wiretap." In other words, the law gives the government the right to wiretap any communication that is assumed to have any relations with terrorist actions. Additionally, under the Act, the government may share information on criminal investigations, including foreign intelligence and counterintelligence. The concept of domestic terrorism refers to: "activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended: (i) to intimidate or coerce the civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States" (the U.S. Patriot Act, Title VII, Sec. 802). Additionally, Section 215 of the Act authorizes the government to petition the FISA Court to compel corporations to disclose their customers' records (Breslow, 2014).

Second, was the amendment to the Foreign Intelligence Surveillance Act of 1978 (FISA 1978), which originally established a surveillance system under which the intelligence agencies,

including the National Security Agency (NSA), were required to submit requests to the FISA Court for intelligence on U.S. citizens. In 2008, Congress passed a law called the FISA Amendments Act (FAA), legalizing the NSA's warrantless wiretapping program and expanding its jurisdiction to gather intelligence from international e-mails and telephone calls of innocent Americans. While racing for the Senate in 2004, Obama had called the Patriot Act "violating our fundamental notions of privacy," and had sponsored a bill to make it harder for federal agents to obtain business records without a court order (Breslow, 2014), and while as a Senate, he had formerly voted against Michael Hayden in 2006, then head of the NSA for his warrantless wiretapping program, as the President, he signed a one year extension of the Patriot Act in 2010 and another four-year renewal of the Act in 2011. Also, in 2008, he voted for the FISA Amendment Act, which expandedthe government's ability to eavesdrop on U.S. citizens without a court order. The amendment included provisions allowing roaming wiretaps and government searches of business records. Obama argued that the renewal was needed to protect the United States from terrorist attacks. The extension sections allowed investigators to get "roving wiretap" court orders which allowed them to follow terrorism suspects who switch phone numbers or providers; to get orders allowing them to seize "any tangible things" relevant to a security investigation and to get national-security wiretap orders against noncitizen suspects who are not believed to be connected to any foreign power (Savage, 2011).

Another piece of legislation easing unwarranted wiretapping was one that permitted the NSA to share the raw communications data it intercepts directly with agencies, including the FBI, the DEA, and the Department of Homeland Security, under Executive Order 12333. Before the new rule, the NSA actually collected data with little oversight, transparency, or concern for privacy, but shared it with these agencies "only after it had screened the data, filtering out unnecessary personal information, including about innocent people" (Tummarello, 2017). Executive Order 12333 was issued in the Reagan administration and made a distinction between the necessary procedures for an "investigation" rather than what is known as a "threat assessment". Accordingly, the term 'investigation' implies the existence of some kind of evidence on a target's being a probable threat and hints at the necessity of further surveillance information to guarantee security. It usually requires a visit to the FISA Court, while extending the definition of a "threat assessment" leads to the IC's permission to conduct surveillance in an 'investigation' situation (Erwin, 2013, in O'Malley, 2016, p. 6). The expansion reduced the risk that the NSA would lose any information that might be valuable to other agencies; yet it increased the likelihood that officials would access innocent people's private information.

The fourth controversial legislation is the Cybersecurity Act of 2012. The Act recognizes that existing legal barriers have prevented the private sector from monitoring even its own systems or those of clients for whom it provides cybersecurity services. According to section 701 of the bill, private companies have permission to monitor and defend their own systems and the systems of a third party who authorizes them to act on its behalf. Section 702 allows private companies to voluntarily share cyber threat information among themselves. The bill also mentions, under Section 703, that there will be at least one "lead Federal cybersecurity exchange" to facilitate and encourage information sharing with both Federal and non-Federal entities. In addition, DHS may, if it wishes, designate additional exchanges that could be operated by Federal or non-Federal entities.

Therefore, FOUR legislative provisions contribute to the stabilization of informational superiority. Surveillance of millions of phone records is being done under Section 215 of the

PATRIOT Act; surveillance of Internet communications internationally is being done under Section 702 of the FISA Amendments Act; and surveillance of communications overseas is done under Executive Order 12333. All four processes were implemented using presidential powers in the current century. Obama extended the Patriot Act twice in 2010 and 2011, voted for the FISA Amendments Act renewal in 2008, invoked Executive Order 12333, pushed the Cybersecurity Act of 2012, and finally issued a Presidential Directive.

Continuation and expansion of big data collection, storage, and analysis programs

The legal permissions paved the way for the expansion of large-scale 'data collection' programs through communication networks targeting Internet users, including American citizens. Though the whole US intelligence community consists of 17 agencies headed by the Office of the Director of National Intelligence (ODNI), much of what takes place and can be traced as an act of securitization is committed by the National Security Agency (NSA) as America's "largest and most secretive intelligence agency, so intent on remaining out of public view that it has long been nicknamed "No Such Agency"" (Risen & Lichtblau, 2005). Founded in 1952, the NSA is now the largest U.S. intelligence organization, providing global monitoring, collection, and processing of information. Under a presidential order signed in 2002, for example, it monitored the international telephone calls and international e-mail messages of thousands of people inside the United States without warrants (Risen & Lichtblau, 2005). The background to these programs dates back to the post-9/11 days when the Information Awareness Office (IAO) was established at the Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense (DoD), headed by retired Admiral John Poindexter, a former National Security Advisor in the Reagan administration. The IAO was created with an official seal depicting a pyramid with an all-seeing eye and the Latin inscription SCIENTIA EST POTENTIA, meaning "science has great potential," or, in other words, "knowledge is power" (Lee, 2015, p. 137). It was created to "develop new tools for detection, classification, identification, tracking, understanding, and preemption" (Lee, 2015, p. 137).

In March 2012, the Obama administration unveiled its "Big Data Research and Development Initiative", building a collaboration between the National Science Foundation (NSF), National Institutes of Health (NIH), the Department of Energy (DOE), U.S. Geological Survey, and Department of Defense (including DARPA). The Executive Office of the President formally announced the initiative on 2012, Mar. 29 and enumerated the following as its objectives:

- Advanced state-of-the-art core technologies are needed to collect, store, preserve, manage, analyze, and share huge quantities of data.
- Harness these technologies to accelerate the pace of discovery in science and engineering, strengthen our national security, and transform teaching and learning; and
- Expand the workforce needed to develop and use Big Data technologies (Executive Office of the President, 2012, p. 1)

Together, the five agencies announced a $200 million commitment "to greatly improve the tools and techniques needed to access, organize, and glean discoveries from huge volumes of digital data" (Executive Office of the President, 2012, p. 1). According to the Executive Order (2012, p. 2), the National Science Foundation was required to implement a comprehensive, long-term strategy containing new methods to derive knowledge from data and develop new approaches for workforce education, including:

- Encouraging research universities to develop interdisciplinary graduate programs to prepare the next generation of data scientists and engineers;
- Funding a $10 million Expeditions in Computing project based at the University of California, Berkeley, that will integrate three powerful approaches for turning data into information - machine learning, cloud computing, and crowd sourcing;
- Providing the first round of grants to support "EarthCube" – a system that will allow geoscientists to access, analyze, and share information about our planet;
- Issuing a $2 million award for a research training group to support training for undergraduates to use graphical and visualization techniques for complex data.
- Providing $1.4 million in support for a focused research group of statisticians and biologists to determine protein structures and biological pathways.
- Convening researchers across disciplines to determine how Big Data can transform teaching and learning.

Also, the DoD was to invest approximately $250 million annually (with $60 million available for new research projects) across the Military Departments in a series of programs to:

- Harness and utilize massive data in new ways and bring together sensing, perception, and decision support to make truly autonomous systems that can maneuver and make decisions on their own.
- Improve situational awareness to help warfighters and analysts and provide increased support to operations (Executive Office of the President, 2012, pp. 2-3).

Accordingly, the government tried to have two types of enhancement in terms of the analytic power of the intelligence system: 1) increase the ability of analysts to infer information from texts in any language; and 2) include more objects and activities any analyst could observe. Among the funded DARPA programs was a key technology applicable to TIA known as Anomaly Detection at Multiple Scales (ADAMS). Another one was the XDATA program, which intended to invest about $25 million annually for four years to develop computational techniques and software tools to process large volumes of data "both semi-structured (e.g., tabular, relational, categorical, meta-data) and unstructured (e.g., text documents, message traffic)" (Executive Office of the President, 2012, p. 3). A third aspect of the initiative concerned bio-surveillance, stating that *the National Institutes of Health* had already gathered and made available data of 200 terabytes on the Amazon Web Services (AWS) cloud under the international 1000 Genomes Project on human genetic variation, which was an example of Big Data (Executive Office of the President, 2012, p. 3).

Also, in June 2013, a *Guardian* article revealed the top-secret PRISM program, leaked by Edward Snowden, an employee of the defense contractor Booz Allen Hamilton at the National Security Agency (Greenwald and MacAskill, 2013a & b). Forty-one PowerPoint presentation slides were leaked, revealing widespread NSA wiretaps on US citizens and worldwide in the form of several surveillance programs. The inauguration of the programs raised media reaction and criticism and resulted in Obama's announcement of a reform in the programs in 2014.

Integration of cyber intelligence information

On Feb. 25, 2015, the Director of National Intelligence (DNI) received an order from President Obama to establish the Cyber Threat Intelligence Integration Center (CTIIC). The order was meant to "connect the dots" regarding foreign cyber threats and cyber incidents

affecting US national interests, and focused on providing all-source analysis of threats to US policymakers (The White House Fact Sheet: CTIIC, 2015). The CTIIC responsibilities include (Presidential Memorandum on the establishment of the CTIIC, 2015):

- Providing an integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests;
- supporting the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force, U.S. Cyber Command, and other relevant United States Government entities by providing access to intelligence necessary to carry out their respective missions;
- oversee the development and implementation of intelligence sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests among the organizations referenced in subsection (b) of this section;
- ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both the United States Government and U.S. private sector entities through the mechanism described in section 4 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity); and
- facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

The establishment of CTIIC can be regarded as a major step in the integration of all information gathered through cyber intelligence. According to Laura Galante (2024), the CTIIC director, the center collects "the best intelligence available—from classified and commercial sources … to help people make better security decisions". The agency was created to ensure that information from intelligence agencies would be shared and that there would be no gaps in datasets.

Discussion

Geopolitics of information and national security requirements

The informational superiority stabilization policy in the Obama administration had at its core details both in terms of aims and means that imply long-term perspectives and objectives to maintain America's informational dominance in the cyber world. This is observable at the national level and within the country's information policy. The decisions to expand cyber intelligence programs relied on U.S. technological assets that enable access to the content of global digital communications, both through data exchanges and via private companies' networks. Continuation and expansion of these programs in his presidency seem to be pragmatic decisions made based on the simple logic that 'when you can do something, why not do it?'. The informational state, according to Braman (2006, p. 314), "knows more and more about individuals, while individuals know less and less about the state". As an informational state, the US information policy involved the maximization of its information power. The process can be analyzed as part of the US cyber strategy when situated within the framework provided by the theory of securitization and the geopolitical analysis of US security priorities in the early 21st century. The analysis sheds light on the non-military aspect of 'cyber-inclusive grand strategy

making' in which perceptions of the strategic environment contribute to the securitization move in the form of informational superiority stabilization in cyberspace.

This is explicable, noting that the US started the 21st century in glory and pride. A decade after the peaceful end of the Cold War, the United States remained the only superpower enjoying a triumphant ideology, the most powerful military, a prosperous economy, and an attractive culture worldwide. Laments by conventional wisdom about American decline after the collapse of the Soviet Union had not come true (Nye Jr, 2004, p. 97). The once-considered probable candidates to replace the USSR as a rival superpower, such as Japan, Russia, Germany, and China, were far from able to catch up with the US. Despite Realists' belief in the "durability of the bipolar system" (Walt, 1987), their pessimist ideas that the US foreign policy would "soon miss the Cold War" (Mearsheimer, 1990, p. 35), Neo-Realists' central claim that "balancing was a substantial feature of great power relations" (Waltz, 1979) and their "unipolar moment" (Layne, 1993, p. 5; Krauthamme, 1990/1991) metaphor to refer to the temporality of the US unipolar dominance, the United States was still enjoying its unique position. Yet, at the onset of the new century, the 9/11 attacks shocked America. The deadly bombings happening on American soil and killing dozens of people created uncertainties about the future security of the United States. The implications of the attacks for the U.S. national security and foreign policy apparatus were a change in its perceptions of the country's security threats and vulnerabilities (Ameli et al., 2019, p. 110). America was not threatened by another superpower, but by *terrorism*. The new enemies were not *nation-states* but armed groups, individuals, and their ideologies. The disaster was that "a transnational terrorist organization [had] killed more Americans than the state of Japan did in December 1941" (Nye Jr, 2004, p. 3). As Darvishi & Hatamzadeh (1392 [2013 A.D.], p. 137) state, this increased the importance of terrorism in European and U.S. security strategies. Moreover, the attacks had global geopolitical implications and reflections (Eta'at & Dabiri, 1395 [2016 A.D.], p. 42).

Threat identification, as the first step of grand strategy making, involved the understanding that cyberspace is a pool of information that makes up the backbone of communication in the new century and can be a potential threat if used by US adversaries: "The very technologies that empower us to create and to build also empower those who would disrupt and destroy" (Obama, 2009). The use of the Internet by adversaries could cause catastrophic damage to U.S. national security, with a strong legacy from the 9/11 experience. According to a 9/11 committee report published in 2004, several failures of the US intelligence agencies were identified as blind spots that could have prevented the 9/11 events. The report documented failures, many of which involved information bugs. It maintained that the CIA had not watch-listed future hijackers, it had not trailed them after they traveled to Bangkok, and had not informed the FBI about one future hijacker's US visa or his companion's travel to the United States. Neither had the agency shared information linking individuals in the *Cole* attack to al-Mihdhar. Also, the Federal Bureau of Investigation (FBI) had failed to take adequate steps in time to find al-Mihdhar or al-Hazmi in the United States, had not linked the arrest of Zacarias Moussaoui, described as interested in flight training for the purpose of using an airplane in a terrorist act, to the heightened indications of attack. The FBI also had not expanded the no-fly lists to include names from terrorist watch lists.

The fact that 9/11 caused significant damage, the principle that it should not be repeated, and the idea that, had sufficient information been gathered and used, it would not have occurred, led to the assumption that gathering as much information as possible could play a preemptive

role against future threats. Cyberspace, as a backbone for information flow, became a repository for data that could be stored and analyzed later. According to Nakashima and Warrick's (2013, in Lee, 2015: pp. 169-170) citation of a former senior US intelligence official, then NSA director Gen. Keith Alexander's rationale behind the surveillance programs was that "Rather than look for a single needle in the haystack, his approach was, 'Let's collect the whole haystack. Collect it all, tag it, store it. … And whatever it is you want, you go searching for it". The US information policy, indeed, preferred a control mechanism and replaced Panopticon[1] intelligence with panspectron ways as a feature of informational states, in contrast to the bureaucratic state (Braman, 2006, pp. 314-315). Braman (2006, p. 315) mentions that in the informational state, "information is gathered about everything, all the time, and particular subjects become visible only in response to the asking of a question" and "the subjects of surveillance never know when, how, or why they might become visible on the panspectral screen". The perception that cyberspace could be used to collect as much information as possible to prevent future attacks was indeed a confrontational way to combat threats to national security. Obama (2014), as the US president, explains the case as follows:

We were shaken by the signs we had missed leading up to the attacks -- how the hijackers had made phone calls to known extremists and traveled to suspicious places. So, we demanded that our intelligence community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack. … It is hard to overstate the transformation America's intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers. Instead, they were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.

But 9/11 was not the sole reason behind the rationale for the conduct of mass surveillance using cyber. The increase in Internet user numbers means that more people can use the technology for various purposes. The Telecommunication Development Sector (ITU-D) ITU website illustrates the increasing trends in the number of individuals' internet usage of mobile cellular phones, and active mobile broadband subscriptions as of 2001 (see Figure 5).

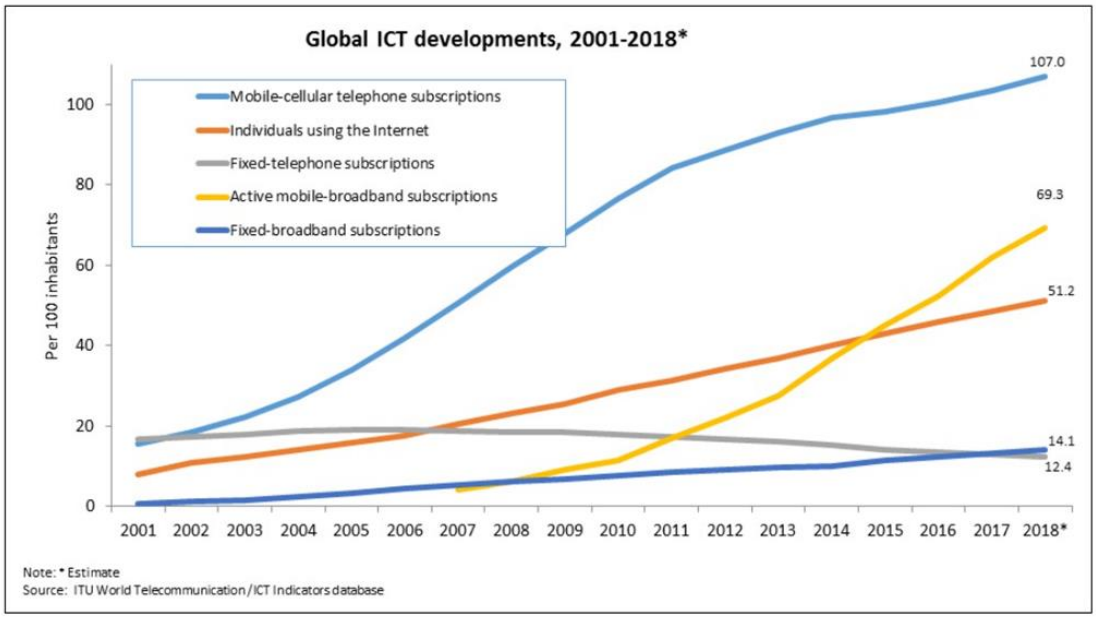

Figure 5: Trends in the number of individuals using the internet, usage of mobile cellular phones, and active mobile broadband subscriptions. Source: ITU, 2019

General perceptions about how the US national security may be threatened and how new technologies could be used by adversaries were themselves strong motivators for the conduct of mass surveillance programs. The value of 'integrated information' to protect the homeland was a generally agreed-upon principle:

We will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information; establish a nationwide framework for reporting suspicious activity; and implement an integrated approach to our counterterrorism information systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government (the NSS 2010, p. 20).

The outcome of such assumptions was the adoption of any available means of confrontation to combat the threats. The logic was that the US has to use its technological assets and tools before others use them against it. Cyberspace is a new environment for information flow, and collected data could help prevent disastrous threats to national security, because detailed information about individuals and their communications provides opportunities to enter their communities, examine their communications from multiple perspectives, analyze their relationships, and predict their behavior. Belief in the preemptive power of technology to preserve national security led to the decision to use the US technological superiority as an asset for data gathering. John P. Holdren, Assistant to the President and Director of the White House Office of Science and Technology Policy, expressed the idea well when talking about the Obama Big Data program:

In the same way that past Federal investments in information-technology R&D led to dramatic advances in supercomputing and the creation of the Internet, the initiative we are launching today promises to transform our ability to use Big Data for scientific discovery, environmental and biomedical research, education, and national security (Holdren, 2012, in Lee, 2015, p. 157).

Obama himself described the US technological capabilities as "unique" and said that "the

power of new technologies means that there are fewer and fewer technical constraints on what we can do" (Obama, 2014). The digital technology, thus, is a national asset the US officials rely upon to preserve their national security.

Yet, a big portion of the technology is in the hands of private corporations. The private sector is where science could translate into technology and, through its R&D units, into industry. Lashgari (1395 [2016 A.D.], p. 118) even argues that Silicon Valley holds geopolitical strategic importance as a major base for managing the Internet. Therefore, public-private cooperation was a substantial element of the surveillance expansion process between 2009 and 2017. A robust private sector is a second national asset the U.S. government leverages for geopolitical and national security preservation in cyberspace. The private sector is more agile at developing new technologies than the government. William Lynn III, former Deputy Secretary of Defense, wrote an article in 2012 in Foreign Affairs:

On average, it takes the Pentagon 81 months to bring a new computer system into operation after it is first funded. … By comparison, the iPhone was developed in 24 months. That is less time than it would take the Pentagon to prepare a budget and obtain congressional approval (Lynn III, 2010).

According to an NSA spokesman, the organization would make use of the private sector capabilities in any way possible: "we engage heavily with the industrial and academic research communities to develop new and innovative technologies to help us in securing critical networks, in exploiting the communications of foreign adversaries and in providing vital foreign intelligence to our warfighters" (n.d. in Maurine, 2018, p. 76). One opportunity for the private sector was access to information and the content of communications, owing to hosting servers and the global communication infrastructure. The perception that 'every event has its hints and signs before it happens and no information should be lost', created the basis for strong public-private cooperation, both in the form of information sharing and technology development. Rog (2018, p. 21) explains how a combination of the mentioned surveillance programs helps the NSA gather every kind of data:

The NSA's surveillance programme for accessing data consists of at least two components: the fibre-optic data-gathering method known as Upstream and the PRISM programme, which allows the NSA to request stored data from nine private internet corporations. This data is then made more comprehensible by a supporting program called XKeyscore. XKeyscore processes 150 databases to produce refined data. BULLRUN helps XKeyscore by breaking the encryption applied to the data by either corporations or Upstream. When all programs work in unison, there isn't a piece of data that the NSA can't process.

Communications of individuals worldwide via the Internet were a potential target of mass surveillance, without any prior detection of criminal activity. This made every individual acting in cyberspace a target of surveillance to maintain informational supremacy. Continuation and expansion of surveillance programs exemplify a pragmatic solution to the security dilemma, or, as Obama said, a "trade off" (Obama, 2013), aimed at balancing security and privacy. Besides the threat perceived from terrorist groups, technological advancements made the 'new' intelligence methods 'inevitable':

The same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach. And at a time when more and more of our lives are digital, that prospect is disquieting for all of us (Obama, 2014).

The premise of the informational superiority stabilization process was the identification of integrated information as a source of power in cyberspace, and of the US as playing a leading role in exerting power and influence in the cyber world. As the home country to the new Information Technologies, the US used its unique position to stand and stay at the top: "The nation that invented the Internet, that launched an information revolution, that transformed the world -- will do what we did in the 20th century and lead once more in the 21st" (Obama, 2009). The four stages of the process of informational superiority stabilization are summarized in Figure 6.

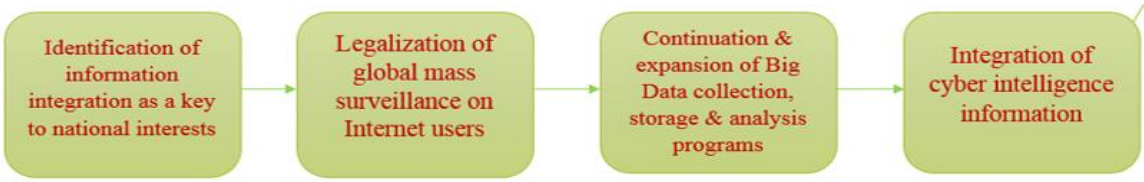

Figure 6: The informational superiority stabilization process

The whole process, named here as informational superiority stabilization, was an exemplification of the US information power maximization and part of the country's information policy, in general. As the author's central argument suggests, the policy predates the Obama administration and is part of the long-term US national security priorities. After Obama, Donald Trump came to the white house with the 'America First' slogan, promising a leading position for the US in almost all areas. The US 2017 National Security Strategy, published during his first term of presidency, reads:

America's ability to identify and respond to geostrategic and regional shifts and their political, economic, military, and security implications requires that the U.S. Intelligence Community (IC) gather, analyze, discern, and operationalize information. … The United States will, in concert with allies and partners, use the information-rich open-source environment to deny the ability of state and non-state actors to attack our citizens, conduct offensive intelligence activities, and degrade America's democratic institutions. … The United States will integrate our analysis of information from the diplomatic, intelligence, military, and economic domains to compete more effectively on the geopolitical stage (The White House, 2017, p. 32).

The document clearly emphasizes the need to gather information from diverse sources for geopolitical purposes. Also, the 2021 Interim National Security Strategic Guidance published under Biden insisted that: "Robust law enforcement and intelligence capabilities, as well as strong cooperation and appropriate information sharing, will be critical to understanding and addressing the broad spectrum of violent extremism America confronts today" (The White House, 2021, p. 19), focusing on the role of information sharing with partners to deal with security threats. The way the policy was implemented is less clear than it was in the first two decades of the century. In fact, most factual details of its implementation were derived from the 2013 Snowden leaks, and no subsequent whistleblowers have disclosed classified information about government eavesdropping on citizens' online communications, other than what the NSA itself disclosed in the aftermath of the Snowden case. As for other stages of the process, i.e., 'legalization of the mass surveillance' and 'information integration', Section 702 of the FISA Amendments Act expanded legal mass surveillance of U.S. citizens in 2024, and the CTIIC continues to operate. In April 2024, the Congress expanded the government's surveillance

powers under section 702 of the Foreign Intelligence Surveillance Act allowing the government "to compel an enormous range of U.S. businesses, organizations, and individuals to assist the National Security Agency" and giving access to "their phones, computers, wifi routers, and other communications equipment through which emails, texts, phone calls are transmitted between Americans and non-Americans overseas" (Rosenfeld & Autery, 2024). The law brought the issue to the attention of the American public for its violation of U.S. citizens' civil liberties, but was ultimately passed by Congress on April 20, 2024. Critics regard the law as providing an "ongoing source of intelligence for domestic investigations" (Toomay & Robinson, 2024). Thus, the basics of the US information policy are believed to be the same as those inferred in this research as "informational superiority stabilization".

Though the policy has been highly controversial for its unlikelihood to create a balance between ensuring national security and protecting individual privacy rights, it is being enacted even more strongly than in the Obama years. Critics argue that it violates the First Amendment and the right to privacy (Issitt & DiLascio, 2024). From a theoretical perspective, Königs (2022, p. 1) argues that mass surveillance raises three potential sources of concern: "(1) the concern that governments diminish citizens' privacy by collecting their data, (2) the concern that they diminish their privacy by accessing their data, and (3) the concern that the collected data may be used for objectionable purposes". But defending the policy, less than a week after Snowden leaks, Obama insisted on the fact that the Congress had been briefed about the policy and also on its inevitability: "… you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society" (Obama, 2013). Controversies continue in the American media about the issue, especially after the 2024 expansion of Section 702 of the FISA, but there seems to be no change in the long-term policy since it is derived from national security concerns.

Conclusion

This manuscript was a case study in the field of sociology of science, i.e., the interplay of sociology and technology. As technological advancements in information sciences increased in the late 20th century, cybersecurity emerged as a new concern, as the exchange of information in cyberspace was perceived as a threat to national security. Using process tracing as the research method, this article analyzed findings on the informational superiority stabilization process within U.S. cyber strategy and information policy during the Obama administration. The objective was to examine how practical securitization of cyberspace was implemented to institutionalize U.S. cyber influence. The process was analyzed in the text relying on a techno-geopolitical analysis of the securitization move in the Obama administration.

As a securitization practice that employs extraordinary measures to preserve security, the steps taken in the process indicate that the pursuit of maximum influence in cyberspace serves as a strong motivator to use all available instruments, including the country's technological superiority and the private sector's capabilities.

Findings indicate a four-stage process in the information policy of the US in the Obama administration, starting with the basic assumption about the significance of 'information integration', rather than dispersing information, and cyberspace communications as a key to national interests. this is significant in that identification of information integration as a key to national security preservation, as a long-lasting premise of state intelligence, was adjusted with the new technological advancements; in that, it was followed by the understanding that cyberspace could be used by the US adversaries for communication, so long-term methods are

needed to use cyberspace to gather information with a preemptive function. The confrontational approach to security threats was fundamentally cyber-inclusive, encompassing the legalization and practice of mass cyber-surveillance programs. Thus, the elimination of legal barriers to mass surveillance was the second stage, followed by the expansion of Big Data collection, storage, and analysis. This means that Cyberspace was taken as the primary site for data collection, given its growing role as the host of most global information flows. The final stage, the establishment of the CTIIC, aimed to integrate all information to prevent data gaps and erroneous decisions. After all, the perception that the US was the world leader and had to be the most influential cyber power underpinned the country's information policy as an auxiliary goal. Pursuit of 'stabilized informational superiority' was indeed at the core of the US cyber policy.

Endnote

1. Panopticon refers to surveillance practices in which the individual subject of surveillance is first identified and then multiple techniques and technologies of observation are directed upon the subject.

References

Ameli, S. R., Hosseini, H. & Noori, F. (2019). Militarization of cyberspace, changing aspects of war in the 21st century: The case of Stuxnet against Iran. *Iranian Review of Foreign Affairs*, 10(1), 99-136. Retrieved from https://irfajournal.csr.ir/article_126485_0e317d545f418eb25a18ee92bd0bc2f0.pdf

Banks, W. C. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Journal,* 66(3), 513-525. Retrieved from https://law.emory.edu/elj/_documents/volumes/66/3/banks.pdf

Beach, D. & Pederson, R. B. (2013). *Process-tracing methods: Foundations and guidelines*. The University of Michigan Press. https://doi.org/10.3998/mpub.10072208

Ben-Israel, I. & Tabansky, L. (2014). An interdisciplinary look at security challenges in the information age. In G. Siboni (Ed.). *Cyberspace and national security selected articles II* (pp. 51-67). INSS Institute for National Security Studies.

Bennett, A. (2010). Process tracing and causal inference. In H. Brady & D. Collier (Eds.), *Rethinking Social Inquiry* (pp. 207-219). Rowman and Littlefield.

Bennett, A. & Checkel, J. T. (2012). *Process tracing: From philosophical roots to best practices*. Simons Papers in Security and Development, No. 21/2012, School for International Studies, Simon Fraser University. Retrieved from https://summit.sfu.ca/_flysystem/fedora/sfu_migrate/14884/SimonsWorkingPaper21.pdf

Braman, S. (2006). *Change of state: Information, policy and power*. The MIT Press.

Braman, S. (2011). Defining information policy, *Journal of Information Policy,* 1(1), 1-5. Retrieved from http://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.1.2011.0001/1610440/jinfopoli_1_2011_1.pdf

Breslow, K. (2014). *Obama on mass government surveillance, then and now. Frontline*. Retrieved from https://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/

Brier, Jr., Th. F. (2017). Defining the limits of governmental access to personal data stored in the cloud: An analysis and critique of Microsoft Ireland. *Journal of Information Policy*, 7, 327-371. https://doi.org/10.5325/jinfopoli.7.2017.0327

Butler, D. L. (2001). Technogeopolitics and the struggle for control of world air routes, 1910-1928. *Political Geography,* 20(5), 635–658. https://doi.org/10.1016/S0962-6298(01)00006-3

Buzan, B. & Hansen, L. (2009). *The evolution of international security studies* (eBook). Cambridge University Press. Retrieved from http://103.214.54.122/repository/The%20Evolution%20of%20International%20Security%20Studies.pdf

Buzan, B. & Little, R. (2000). *International systems in world history: Remaking the study of international relations*. Oxford University Press.

Buzan, B., Wæver, O. & de Wilde, J. (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner.

Cavelty, M. D. (2007). *Cyber-security and threat politics: Us efforts to secure the information age* (eBook). Taylor & Francis e-Library. Retrieved from http://opac.lib.idu.ac.id/unhan-ebook/assets/uploads/files/530d1-cyber-security-and-threat-politics.pdf

Cayford, M. & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society,* 34(2), 88-103. https://doi.org/10.1080/01972243.2017.1414721

Choucri, N. & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists,* 68(2), 70–77. https://doi.org/10.1177/0096340212438696

Choukri, N. (2015). *Explorations in cyber international relations: A research collaboration of MIT and Harvard University*. Massachusetts Institute of Technology Political Science Department, Research Paper No. 2016-1. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2727414

Clement, A. & Obar, J. A. (2016). Keeping Internet users in the know or in the dark: An analysis of the data privacy transparency of canadian internet carriers. *Journal of Information Policy*, 6, 294-331. https://doi.org/10.5325/jinfopoli.6.2016.0294

Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure (2009). Cybersecurity & Infrastructure Security Agency. Retrieved from https://irp.fas.org/eprint/cyber-review.pdf

Darvishi, F. & Hatamzadeh, A. (2013). The process of US and EU confrontation with terrorism from different perceptions to collaboration. *International Quarterly of Geopolitics*, 9(2), 136-160. https://doi.org/20.1001.1.17354331.1392.9.30.5.8[in Persian].

Deeks, A. (2015). An international legal framework for surveillance. *Virginia Journal of International Law,* 55(2), 291-368. https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegalFramework.pdf

Dunn, M. (2005, July). A Comparative Analysis of Cybersecurity Initiatives Worldwide. In *WSIS Thematic Meeting on Cybersecurity* (pp. 1-32). International Telecommunications Union. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Emmers, R. (2016). Securitization. In A. Collins (Ed.), *Contemporary Security Studies* (Fifth ed., originally in 2007) (pp. 168-181). oxford university press.

Etaat, J. & Dabiri, A. A. (2016). study of the spatial dimensions of terrorism. *International Quarterly of Geopolitics*, 12(42), 24-47. Retrieved from https://journal.iag.ir/article_55768_9a528a23ec4a4ffee7bc553b5922fdc1.pdf?lang=en

Executive Office of the President. (2012, Mar. 29). Obama Administration Unveils "Big Data" Initiative: Announces $200 Million in New R&D Investments. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/11/19/release-obama-administration-unveils-big-data-initiative-announces-200

Friedman, B. & Hendry, D. G. (2019). *Value sensitive design: Shaping technology with moral imagination*. The MIT Press.

Fuerth, L. (2009). Cyberpower from the presidential perspective. In F. D. Kramer, S. H. Starr, and L. K. Wentz, *Cyberpower and National Security* (pp. 557-562). Center for Technology and National Security Policy, National Defense University Press, Potomac Books Inc. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

Galante, L. (2024, Dec. 12). Laura Galante, Intelligence Community's Cyber Executive and Director of the Cyber Threat Intelligence Integration Center (CTIIC), Office of the Director for National Intelligence, United States [Interview/ Interviewer: A. R. Choudhury]. Retrieved from https://govinsider.asia/intl-en/article/laura-galante-intelligence-communitys-cyber-executive-and-director-of-the-cyber-threat-intelligence-integration-center-ctiic-office-of-the-director-for-national-intelligence-united-states

Gilchrist, A. (Ed.). (2009). *Information science in transition*. Facet Publishing.

Gill, A. (2018). Data surveillance: Need for a policy to achieve equilibrium between state and individual interest. *Nirma University Law Journal*, 6(2), 57-69. https://ssrn.com/abstract=3442993

Greenwald, G. & MacAskill, E. (2013a, Jun. 7). NSA prism program taps in to user data of apple, Google, and others. *The Guardian*. Retrieved fromhttps://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., & MacAskill, E. (2013b, Jun. 11). Boundless informant: the NSA's secret tool to track global surveillance data. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Herrera, G. L. (2006). *Technology and international transformation: The railroad, the atom bomb, and the politics of technological change.* State University of New York Press.

Holt, J. & Malčić, S. (2015). The privacy ecosystem: Regulating digital identity in the United States and European Union. *Journal of Information Policy*, 5, 155-178. https://doi.org/10.5325/jinfopoli.5.2015.0155

Issitt, M. L. & DiLascio, T. M. (2024). *Government surveillance: overview. ebsco knowledge advantage*. Retrieved from https://www.ebsco.com/research-starters/law/government-surveillance-overview

ITU (2019). Trends in the number of individuals using the internet, usage of mobile cellular phones, and active mobile broadband subscriptions. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Jones, K. M. L., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A. & Robertshaw, M. B. (2020). "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology*, 71(9), 1044–1059. http://dx.doi.org/10.2139/ssrn.3565553

Kiernan, C. J. & Mueller, M. L. (2021). Standardizing security: Surveillance, human rights, and the battle over Tls 1.3. *Journal of Information Policy*, 11, 1-25. https://doi.org/10.5325/jinfopoli.11.2021.0001

Königs, P. (2022). Government surveillance, privacy, and legitimacy. *Philosophy & Technology*, 35(8), 1-22. https://doi.org/10.1007/s13347-022-00503-9

Krauthamme, Ch. (1990/1991). The unipolar moment. *Foreign Affairs,* 70(1), 23-33. https://doi.org/10.2307/20044692

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr and L. K. Wentz (eds) *Cyberpower and National Security* (pp. 24-42). Center for Technology and National Security Policy, National Defense University Press, Potomac Books Inc. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

Lashgari, E. (2016). Explanation of the strategic importance of cyber space management and geographic zone control. *International Quarterly of Geopolitics,* 12(2), 105-123. https://dor.org/20.1001.1.17354331.1395.12.42.5.3 [in Persian]

Layne, Ch. (1993). The unipolar illusion: Why new great powers will rise. *International Security*, 17(4), 5-51.

Lee, N. (2015). *Counterterrorism and cybersecurity. Total information awareness* (2nd Ed.). Ebook. https://doi.org/10.1007/978-3-319-17244-6

Lynn III, W. F. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs,* 89(5), 79-108. Retrieved from https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Marandi, M. & Halalkhor, M. (2016). America and the securitization of Iran after the Islamic Revolution, 1979-2013: Continuation or change? *International Quarterly of Geopolitics,* 11(40), 85-116. https//dor.org/20.1001.1.17354331.1394.11.40.4.1

Maurine, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press. Retrieved from https://books.google.com/books?id=rKpCDwAAQBAJ&pg=PA76&lpg=PA76&dq=us+cybercom+budgets+comparison&source=bl&ots=SYqoGakSpS&sig=ACfU3U2Qc5D7nq3sjTEaEVYbnFcylfVP6A&hl=en&sa=X&ved=2ahUKEwjDz8eQ8r_oAhUO1RoKHat4CCUQ6AEwGHoECAoQAQ#v=onepage&q=us%20cybercom%20budgets%20comparison&f=false

McCarthy, D. R. (2013). Technology and 'the international' or: How I learned to stop worrying and love determinism. *Millennium: Journal of International Studies,* 41(3), 470–490. https://doi.org/10.1177/0305829813484636

McCarthy, J. A., Burrow, Ch, Dion, M. & Pacheco, O. (2009). Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. In F. D. Kramer, S. H. Starr and L. K. Wentz (eds) *Cyberpower and National Security* (pp. 543-556). Center for Technology and National Security Policy, National Defense University Press, Potomac Books Inc. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

Mearsheimer, J. J. (1990). Why we will soon miss the cold war. *The Atlantic Monthly*, 266(2), 35-50. Retrieved from https://www.theatlantic.com/past/politics/foreign/mearsh.htm

Misa, T., J. (2008). Transforming the international system: Geoffrey L. Herrera's Technology and international transformation. *Technology and Culture,* 49(1), 230-233. https://doi.org/10.1353/tech.2008.0028

National Security Strategy (NSS) (2010, May). Washington: The White House. Retrieved from http://nssarchive.us/NSSR/2010.pdf

Nye Jr., J. S. (2004). *Power in the Global Information Age: From Realism to Globalization*. Routledge, Taylor & Francis.

Nye Jr, J. S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs. Harvard Kennedy School. Retrieved from https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

O'Malley, C. (2016). *The cyber-industrial complex*. Political Science Senior Thesis. Bemidji State University. Retrieved from https://www.bemidjistate.edu/academics/political-science/wp-content/uploads/sites/40/2022/03/Omalley-Final.pdf

Obama, B. (2009, May 29). Remarks by the President on securing our nation's cyber infrastructure. The White House. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Obama, B. (2013, Jun. 7). Statement by the President. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president

Obama, B. (2014, January 17). Remarks by the President on review of signals intelligence. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Peirce, C. (1955). Abduction and Induction. In J. Buchler (Ed.), *Philosophical Writings of Peirce* (pp. 150-156). New York: Dover Publications Inc.

Presidential memorandum: Establishment of the CTIIC. (2015, Feb. 25). The White House Office of the Press Secretary. Retrieved from https://www.dni.gov/files/CTIIC/documents/CTIIC-Presidential-Memorandum.pdf

Rifkin, J. (2011). *The third industrial revolution: How lateral power is transforming energy, the economy, and the world*. London: Palgrave Macmillan. Retrieved from https://edisciplinas.usp.br/pluginfile.php/8754049/mod_label/intro/epdf.pub_the-third-industrial-revolution.pdf

Risen, J. & Lictblau, E. (2005, Dec. 16). Bush lets U.S. spy on callers without courts. *The New York Times*. Retrieved from https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

Rog, J. (2018). *Updating securitization to the age of information: Revisiting security sectors by examining PRISM.* Bachelor's Thesis. Retrieved from https://studenttheses.uu.nl/handle/20.500.12932/31079

Rosenfeld, D. & Autery, R. (2024). *Senate approves massive expansion of government surveillance power; Brennan Center reacts*. Brennan Center for Justice. Retrieved from https://www.brennancenter.org/our-work/analysis-opinion/senate-approves-massive-expansion-government-surveillance-power-brennan

Savage, Ch. (2011, May 19). *Deal reached on extension of Patriot Act*. The New York Times. Retrieved from https://www.nytimes.com/2011/05/20/us/20patriot.html

The National Intelligence Strategy of the United States of America (2009). Washington: Office of the Director of National Intelligence. Retrieved from https://climateandsecurity.org/wp-content/uploads/2019/01/national-intelligence-strategy-2009.pdf

The National Intelligence Strategy of the United States of America (2014). Washington: Office of the Director of National Intelligence. Retrieved from https://climateandsecurity.org/wp-content/uploads/2019/01/national-intelligence-strategy-2014.pdf

The White House (2017). *National Security Strategy of the United States of America*. Retrieved from https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

The White House (2021). *Interim national security strategic guidance*. Retrieved from https://nssarchive.us/wp-content/uploads/2021/03/2021_interim.pdf

The White House Fact Sheet (CTIIC) (2015). Washington: Office of the Press Secretary. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

Toomay, P. & Robinson, S. (2024 June). Mass surveillance is dangerous for American communities: Reforming the section 702 spying regime. *Human Rights Magazine*. Retrieved from https://www.americanbar.org/groups/crsj/resources/human-rights/2024-june/mass-surveillance-dangerous-american-communities-reforming-section-702/

Tummarello, K. (2017, January 12). *Obama expands surveillance powers on his way out*. *Electronic Frontier Foundation (EFF)*. Retrieved from https://www.eff.org/deeplinks/2017/01/obama-expands-surveillance-powers-his-way-out

USA Patriot Act. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*. Public Law 107–56 —OCT. 26, 2001. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

Walt, S. (1987). *The Origins of alliances*. Cornell University Press. retrieved from https://api.pageplace.de/preview/DT0400.9780801469992_A29967168/preview-9780801469992_A29967168.pdf

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley Publishing Company. Retrieved from https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf

Yannakogeorgos, P. A. (2009). *Technogeopolitics of militarization and security in cyberspace.* Doctoral Thesis. Rutgers University. Retrieved from https://rucore.libraries.rutgers.edu/rutgers-lib/26118/PDF/1/