2020

A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Gokhan Ikitemur

Andy Igonor
Franklin University, andy.igonor@franklin.edu

A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies

Gokhan IKITEMUR[a,1], Bilge KARABACAK[b] and Andy IGONOR[b]
[a] *Freelance Security Consultant, Ankara, Turkey*
[b] *Ross College of Business, Franklin University, Columbus, OH*

Abstract. Governments today emphasize space systems as critical infrastructures. Many vital services, including communications, transportation, and maritime operations, depend on space systems. Cyber systems represent an essential component that enables effective functioning, configuration, and monitoring of technological space services. Space systems possess unique vulnerabilities and properties that attract the attention of hackers, and often with varying motivations. The private sector increasingly participates in the production of space technologies, and as a result of the differences in perceptions and priorities of governments and the private sector, handling the challenges of governance as it relates to the cybersecurity of space systems presents an avenue for research. Public-private partnership is one effective way of solving this governance challenge that public and private entities face. With several possible approaches to building a workable partnership between the public and private organizations, this paper offers a mixed approach with the potential to improve the security of space systems, mitigate vulnerabilities, and run effective campaigns against cyber threats.

Keywords. Critical Infrastructures, Space Systems, Cybersecurity, Dual-use, Public-Private Partnership, Regulations, Government Incentives

1. Introduction

Critical infrastructures are vital assets for public safety, economic welfare, and national security of countries. According to the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", an industry can be defined as "critical" if damage or unauthorized access to that system could reasonably:

a. result in the interruption of life-sustaining services,
b. cause catastrophic economic damages, or
c. cause severe degradation of national security [1].

The term critical infrastructure was first used within Executive Order 13010 in 1996 [2]. Since then, governments have always considered cyber threats as one of the prominent risk actors against critical infrastructures [3]. Although critical infrastructures existed long before the Internet and the widespread use of cyber technologies, Critical Infrastructure Protection is defined as an essential governmental term because of the dominant use of cyber systems in infrastructures. Cyber threats are asymmetric; attackers

[1] Corresponding author, E-mail: gokhanikitemur@gmail.com, Akdeniz Cad., Dere Sok., No: 179/11 Umraniye, Istanbul, TR

can hide their acts easily, and compared to conventional threats, cyber threats are extraordinarily cheap and prevalent. Therefore, cyber threats quickly and effortlessly pave the way for harmful attacks against critical infrastructures. There are many materialized cyber attacks against critical infrastructures, including nuclear plants, electrical grids, sewing infrastructures, flight control systems, and harbors [4], [5]. As a result, cyber resilience of critical infrastructures forms a protruding portion of the national security efforts of countries.

Cybersecurity is an essential part of the growing security-related concerns of space infrastructure, including satellites, ground stations, and data links at national, regional, and international levels. There are a lot of critical systems and applications that depend on space technologies such as communications, air transport, and navigation systems, financial and business services, agriculture, transportation, maritime weather and environmental monitoring, and military defense systems. Many critical infrastructures depend on space infrastructures, and space infrastructure, in turn, depends on cyber systems. Furthermore, societies' current substantial and ever-increasing reliance on space technologies has turned potential vulnerabilities of space infrastructure in the face of cyber threats, into major national and international security concerns [6] that need to be addressed at both national and international levels. Given the inextricable linkage between space and cybersecurity, cyber threats against satellites and other space assets are often overlooked in critical infrastructure literature [7]–[9].

This paper principally draws on research conducted from two Ph.D. studies. The first Ph.D. dissertation is titled “Enhancing Cyber Security in Turkey through Effective Public and Private cooperation” written by Gokhan Ikitemur. The second study is titled “Developing and Verifying a Set of Principles for the Cyber Security of the Critical Infrastructures of Turkey” written by Bilge Karabacak. This paper has four sections. The first section is the introduction. The second section covers the general security posture and vulnerabilities of, and cyber threats against space systems. The second section also shares the implications of private sector involvement in space systems and technologies. The third section provides the details of different approaches towards Public-Private Partnerships and suggests a mixed approach for space systems cybersecurity. The fourth section concludes the paper.

2. Background

This section offers a discussion of cyber vulnerabilities and threats associated with space systems. Following this is a discussion of the implications of private sector involvement into space systems. The paper posits that the participation of the private sector brings not only new opportunities but also new challenges in the domain.

2.1. General Security Posture and Vulnerabilities of Space Systems

It would not be wrong to say that the potential exploitation of space systems vulnerabilities by cyber threats is not a new phenomenon. Today, as space systems become critical to all components of national and international infrastructure, the recognition of cyber risks and vulnerabilities is a matter of necessity. Cyber vulnerabilities of space-based capability is a source of growing concern for national security [8], [10], [11]. Unfortunately, the cybersecurity of space systems and assets are not emphasized enough within the policy domain. When the national space security policies of countries with advanced cybersecurity capabilities are reviewed, it is observable that these countries do not perform well in terms of analysis and identification

of cyber risks against space-based assets, as well as the mitigation of risks to protect these assets.

In comparison to other digitized critical infrastructure, such as energy grids, space-related assets appear more vulnerable to cyberattacks; thus, potentially hindering economic prosperity and endangering societies [7], [8]. Except for some more modern systems such as the European Galileo, civilian applications of widely used space technologies, such as the Global Navigation Satellite Systems are relatively insecure, as they have not been designed with security in mind, given that the space race began only in the 1950s with the launch of Sputnik. Exacerbating current security concerns, digitalization of space assets has increased to a level that a highly sophisticated and well-resourced cyberattack to space assets can cripple national and international capabilities [8]. Moreover, the fact that cyberspace is still a growing field with its deficiencies and inconsistencies, the potential impact of vulnerabilities have worsened and widened.

According to the Livingstone and Lewis, although the level of national cybersecurity readiness for many countries has increased and their overall cybersecurity approach has become more active, "the conjunction of cyber and space remains vulnerable to exploitation in the context of complex and internationalized supply chains and space-related infrastructure". Livingstone and Lewis further claim that space activities' vulnerability to cyberattack lagged behind the other areas in the field of cybersecurity because the challenge is generally overlooked in cybersecurity discussions [8]. For example, although roles and responsibilities for securing outer space and cyber domain are increasingly converging [12], at the UN where threats to nations states are dealt with at the highest level, UN governmental group of experts (GGE) 's including outer space and on cyberspace, have not adequately addressed such a convergence in their respective agendas [8].

2.2. Cyber Threats against Space Systems

Space assets are dramatically becoming more attractive for adversaries, especially as the critical functions associated with them exponentially increase in a growing number of national critical infrastructure systems. Furthermore, goods and services provided through space assets and technologies in our daily lives have increased rapidly, further stimulating economic growth worldwide. As states' dependency on space technologies increases, governments need to provide space-based critical systems with a high level of cyber protection. This is particularly vital for developed states as well as countries with similarly reported or known vulnerabilities [8], [13].

Potential adversaries that are likely to exploit current space-related cyber vulnerabilities can vary in motivation and goals. They can be:

a) Nation-states seeking to maximize their national interests through several ways such as stealing intellectual property and gaining a military advantage,
b) Well-resourced organized crime groups aiming to obtain financial gains,
c) Terrorist organizations with sophisticated capabilities striving to promote their illicit causes, and
d) Talented individuals desiring to achieve their differing personal agenda.

There are indications of alarming situations in which cyber actors threaten the conjunction of space and cyber. Three examples are noteworthy: firstly, any sophisticated adversary can take over a satellite and turn it into a space weapon by merely changing in its orbit. Collision with another satellite will potentially follow this. Such

collision will create space debris that may also pose critical risks for other satellites. Secondly, although with highly asymmetrical results, the US Department of Defense's 2018 auditing exercise showed that its ballistic missile defense systems possessed internal control weaknesses that could be exploited through cyber tools. Such interference via cyber tools targeting the control systems of these missile systems may result in loss of life [13]. Thirdly, according to the 2014 US National Oceanographic and Atmospheric Administration report, its Satellite Data Information System was targeted by hackers, and it was taken offline for almost 48 hours in September 2014 [10].

Cyber threats with diverging interests and capabilities are expanding and transforming at an unprecedented speed, and they encompass space systems. There are several reasons for this expansion and transformation. First, the functioning of modern satellite systems is increasingly reliant on cyber technology. Internet-based networks are used in space assets, including the operation of satellites. This connection can turn those assets into "devices on the Internet of Things" [12]. This also makes space assets more accessible and vulnerable from anywhere in the world to any adversary with access to the Internet. Cyberattacks targeting a satellite's controls, reliability, or bandwidth availability would pose a compelling challenge to critical national infrastructure [14]. Another factor that complicates the challenge is that space-based technologies are highly essential for the provision of data and services in air, land, cyber, and sea domains. Thus, any failure caused by adversaries to space infrastructure will have the potential to cascade to other domains. As previously stated, "insecurity-by-design" is a big challenge. As digital technologies become more of a fundamental part of space-dependent capabilities, and space-based assets' connectivity to the Internet and other public networks increases, adversaries will be able to find new avenues through these vulnerabilities in order to infiltrate space systems [13].

Consequently, space systems insecurity is a direct challenge to critical national assets and national security [13]. These challenges have created opportunities for adversaries to launch high-impact attacks on state-owned strategic assets. The asymmetric nature of cyber threats will be in favor of less developed nation-state adversaries, terrorist groups, and other actors such as organized criminals, and will continue to enable them to attack the nation-states that have a much higher reliance on digital technologies [13]. Besides, the effect of propagating failures caused by cyber threats will increase because of increasing critical interdependencies between space systems and other domains.

2.3. Implications of Private Sector Involvement into Space Systems and Technologies

Space is becoming a more "congested, contested, and competitive" area where an ever-increasing number of actors other than nation-states such as international organizations, and private sector companies are being represented [11]. New actors entering the game will inevitably complicate already existing cybersecurity concerns of national actors in the space domain. Cyber-related governance challenges between the private sector and the public sector will be another point of concern in this new frontier. In a 2017 National Infrastructure Advisory Council (NIAC) study, it was revealed that US governmental entities have exceptional cybersecurity capabilities that are crucial in cyber defense of critical infrastructure. However, the effectiveness of these entities' is constrained mainly because private sector awareness of these capabilities is limited. It is currently highly probable that such governance challenges will be repeated in the cyber domain [15].

Today, an essential share of Internet-dependent critical infrastructures, such as telecommunications, energy, and transportation are privately owned [16]. Although we can use existing models that promote public-private cooperation to protect critical infrastructure assets for space systems, many challenges such as to what extent government institutions can share information with the private sector are still an open debate item. Furthermore, it is still unclear as to what extent governments could consider regulating the private sector, especially urging them to make certain cybersecurity investments. In turn, it is also not clear to what extent such government measures may hinder the private sector's dynamism and creativity. Another possible question relates to what extent the private sector could be held accountable when a cyber-breach or potential misconduct cause harm to civilians. These are governance challenges that need to be solved in order to protect space-based critical assets adequately.

Technological advances lower costs of space activities, paving the way to an influx of market forces into this domain. Today the space market is estimated to be worth £125 billion. Furthermore, the global space-enabled market is projected to be as big as approximately £400 billion by the year 2030 [17]. Private satellite services contribute to several sectors from agriculture, transportation, maritime to environmental monitoring. The growing reliance on commercial satellites has reached the extent that some of the military requirements are met by private sector capabilities [9]. The commercial use of space will enhance productivity, increase efficiency and effectiveness, and lower costs in many sectors. This process, however, will lead to the marketization of the space domain that will potentially harm inadequate efforts to protect critical space assets against cyber threats. With the increased participation of private entities into space efforts by using cutting-edge technologies, the private sector will capitalize on highly sensitive and valuable data that will be targeted by adversaries especially for cyber espionage in order to steal intellectual property.

The analysis of the US' Public-Private Partnership over the last 20 years reveals some positive progress. A US General Accounting Office (2002) report pointed out that although the growing importance of satellites requires further protection, government efforts on national critical infrastructure protection did not include the satellite industry [18]. Furthermore, there was no suggestion in the 2002 version of the US National Strategy for Homeland Security to include the satellite industry in the nation-wide approach to protecting critical infrastructures from the entities that are responsible from securing those assets against cyber threats [19]. According to the 2017 National Security Strategy report, government entities will cooperate with the space industry to enhance the resilience of the US's space architecture [20]. When necessary, the US government will consider covering private sector companies with national security protections. However, there is no provision for establishing any mechanism to carry out such a task.

Private sector companies have an incentive to minimize their costs and innovate rapidly. Characteristically, the private sector will seek maximum profit in space, most probably at the sacrifice of necessary cybersecurity measures to protect space assets. Therefore, it is likely that cybersecurity will not be a primary concern in private-sector's space activities, especially in a time when market forces are starting to dominate space [12]. This characteristic feature of the private sector is profoundly incompatible with the realities of cyber and space fields, as cyber threats become imminent. On the other side of the coin, there is no clear information regarding to what extent private sector owned critical space assets have been a victim of such attacks, as the private sector is ever concerned that public disclosure of a security breach could potentially ruin their companies' reputation and result in liability issues [7]. According to the results of the

2017 Black Hat Survey, IT and security professionals from more than 15 European countries are convinced that a cyber attack will breach critical infrastructure across multiple countries and that an attack with huge impact will occur within the next two years [21]. Another striking revelation comes from the Council on Foreign Relations' Preventive Priorities Survey 2019. The attendees, who are government officials, foreign policy experts, and academics, ranked the threat of a highly disruptive cyberattack on the US critical infrastructure and networks as the utmost concern to homeland security [22].

National actors have been increasingly facilitating the private-sector adaptation of dual-use technologies in space [12]. These technologies are also increasingly becoming a response to the shrink in national defense budgets [23]. Although there is no generally accepted definition of dual-use [24], the term "dual-use technologies" are used to denote civilian applications that can also be used for military purposes [25]. The main difficulty for dual-use technologies is that they can be exploited beyond their initial applications [26]. Initially, there was a determination to separate military space systems from commercial and civilian assets regarding their development and operation. This determination has eroded in the face of private sector's success that not only caused a decrease in defense expenditures but also reached a level that has proved itself as effective as military technology especially when it comes to the capture and analysis of satellite imagery [13]. For instance, the US reliance on private sector assets for military purposes increased by almost 560 percent during the Iraq war of 2003 [27]. However, the dual-usage of space-related technologies increase risks by further blurring line between 'military' and 'civilian' activities in cyber and space, having complicated repercussions in both domains. According to Baylon (2014), taking into consideration the dual use of those technologies, it becomes challenging to determine whether a space asset is developed only for civilian purposes, or whether this asset enables a military application as well. This, in turn, might provoke other actors in space to improve their space capabilities. Lack of clarity in terms of which critical space asset is used as a war component can result in adversaries targeting civilian assets in warfare. Therefore, adversaries could aim to wreak havoc not only on strategic weapons systems but also on civilian space assets. The blurring line between 'military' and 'civilian' applications at this juncture could also undermine deterrence and strategic stability as it causes uncertainty and confusion. In such environments, cyber offense prevails cyber defense as the former is technologically easier and more cost-effective than the latter [8], [26]. This will make offensive actions rather than defensive measures in the cyber and space arena the acceptable behavior. Justification of offensive behavior under the guise of defensive ones will diminish mutual trust and harm strategic decision-making processes as the risk of deception among actors in the space domain. If the threat landscape fosters an ambiguity of intent for state actions, even peaceful state actions such as commercial use of a satellite may trigger suspicion among other states. After construing another state's actions as offensive, states will increase their perceived threat level. This will, in turn, contribute to the escalatory cycle. This circle finally will culminate in the militarization of the space and cyber fields. A potential cyber arms race in space is not the future that will best serve the parties in space [11], [28].

The transformation is unfolding in this junction, where cyber meets space levels the playing field in a way that the public and private sector is not organized to respond appropriately. Policymakers and the space industry struggle to grasp the full implications of cyber threats in the context of both cyber and space-related critical assets. Because of the growing interconnectedness and interdependence between the cyber and space sectors, there is a need to apply measures other than applying higher-grade military

hardening and cyber defense measures to civilian and commercial space assets with the capability of supporting military applications [12]. Securing critical national infrastructure would not only enhance the level of civilian preparedness and resilience but also it would help to minimize risks and threats facing governments in both cyber and space domains [13]. These measures are detailed in the next section.

3. A Mixed Public-Private Partnership (PPP) Approach for Space Systems Cybersecurity

Before focusing on the possible PPP incentives between the government and the private sector, it should be emphasized that the private sector needs to be aware that their decisions and ability to maintain organizational security could directly impact public vulnerability. For that reason, when protecting critical infrastructures like space systems, corporate owners should focus not only on organizational costs, but also on the potential "social costs" in the event of a cyber attack [29]. PPP is one of the essential instruments for the private sector to ensure an inclusive focus on costs. The other side of PPP is that "the state is incapable of providing the public good of security on its own" [30]. It is also argued that governments are unlikely to achieve high levels of cyber defense and resilience without resorting to PPPs [31]. As a result, PPP is one of the essential mechanisms to facilitate space systems' cybersecurity collaborations between the governments and private actors.

The U.S. 2010 National Security Strategy places particular emphasis on PPPs and exhorts the executive branch to collaborate with the private sector. Government agencies such as the Department of Defense (DOD), the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (DNI), and the State Department are working to deliberately harness the private sector's capabilities in their efforts to achieve national security [32]. The same remains applicable to the EU. In his 2013 study, Irion focuses on Network and Information Security (NIS) governance in the EU and examines cooperation between public and private organizations that operate information and communications technology (ICT) networks. He concludes that effective NIS governance can be achieved by taking advantage of PPPs together with clearly-defined governance mechanisms. There are three distinct approaches to facilitate PPP. Hathaway and Klimburg argue that the way to encourage private businesses to adopt a "whole-nation-approach" is to provide them with various incentives, ranging from enhanced security support to indirect commercial benefits [33]. The other approach is the regulation of the private sector. Even though commercial instruments can motivate private businesses to join forces with the state, many governments generally prefer legal means such as regulations to coerce their subjects [34]. Stavridis and Farkas define public-private collaboration as a voluntary interaction between governments and private organizations to achieve resource efficiency. According to the authors, cooperation with the private sector does not necessarily involve financial transactions or even contracts; it can be entirely voluntary [32]. Lewis argues that while strict government regulation is necessary for such fields as banking, commerce, and transportation when it comes to regulating cyber domains, a voluntary partnership model suffices [35]. Some experts oppose the voluntary approaches for PPP as the primary means of enhancing resiliency and cybersecurity; they argue that governments should utilize regulatory measures to fully take advantage of available resources [36], [37]. In a white paper jointly prepared by Business Software Alliance, Center for Democracy & Technology, US Chamber of Commerce, Internet Security Alliance, and TechAmerica, more cyber regulations mean

more burdens for American companies in the private sector, rendering them uncompetitive in the marketplace. As a result, they claim that hierarchies must be replaced with alternate structures capable of promoting security, competition, and collaboration across multiple fronts [38].

Authors of this paper argue three factors make the voluntary participation of the private sector inefficient. These factors are:

a. The private sector is an indispensable actor in the development of space systems,
b. Cybersecurity of space system is an emerging and critical national security domain,
c. Space systems are critical assets within the scope of nations and a domain of competition in the international context.

As a result, the private sector's participation in space systems' cybersecurity should not be a voluntary matter. Otherwise, it may not engage to the full extent possible, and cybersecurity efforts of space systems could resultantly fail. Nevertheless, government regulation should not be the only approach for cybersecurity efforts of space systems. Instead of strong regulatory approaches, a blend of approaches can be more efficient. For example, Clinton argues that the government should compensate private businesses for cybersecurity investments exceeding their commercial needs [39]. An essential benefit of adopting a mixed approach would be to refrain from the possible failures of voluntary PPPs. Even if they can function as successful networks, PPPs are not flawless structures in and of themselves. PPPs can be limited in addressing complex challenges due to their lack of strong leadership and clear policy goals [40].

Similarly, a 2008 report by the Center for Strategic and International Studies (CSIS) entitled "Securing Cyberspace for the 44th Presidency" points out that many cybersecurity PPPs have suffered because of poorly defined goals and objectives, as well as from a lack of coherently defined strategies and partnership plans [41]. In a recent study that measures the organizational variables associated with cybersecurity preparedness, insufficient government guidance is one of the factors that contribute to the organizational barrier for making cybersecurity preparation [42]. As a result, a mixed approach, incorporating both incentives, government leadership, and voluntary actions could be useful in space system cybersecurity efforts.

4. Conclusion

As the private sector increasingly participates in the production of space technologies, some governance challenges arise, and they may affect the cyber resilience of space systems. Almost all nations emphasize the importance of Public-Private Partnerships within national cybersecurity strategies. Partnerships between public and privates entities should be created for cybersecurity of space systems as well because PPP is an effective way of solving the governance challenge among public and private entities. However, there are several approaches to building a partnership between public and private organizations, and there are some disputes regarding which method should be used for national cybersecurity efforts. In this paper, a mixed PPP approached is suggested to improve cybersecurity space systems, mitigate vulnerabilities, and run effective campaigns against cyber threats. By this combined approach, both voluntary participation, government incentives, and government regulations should be effectively and harmoniously employed.

References

[1] USA, *USA Patriot Act*. USA, 2001, pp. 1–132.

[2] The White House, *Executive Order 13010 - Critical Infrastructure Protection*. USA: The White House, 1996, pp. 37345–37350.

[3] U. Tatar, B. Karabacak, and Adrian Gheorghe, "An Assessment Model to Improve National Cyber Security Governance," in *11th International Conference on Cyber Warfare and Security*, 2016, pp. 312–319.

[4] S. M. Condron, "Getting It Right: Protecting American Critical Infrastructure In Cyberspace," *Harv. J. Law Technol.*, vol. 20, pp. 403–422, 2007.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Surviv. Glob. Polit. Strategy*, vol. 53, no. 1, pp. 23–40, 2011, doi: 10.1080/00396338.2011.555586.

[6] HM Government, "National Space Security Policy." UK Government, Apr-2014.

[7] G. Falco, "Job One for Space Force: Space Asset Cybersecurity." Harvard Kennedy School, Jul-2018.

[8] D. Livingstone and P. Lewis, "Space, the Final Frontier for Cybersecurity?" Chatham House, Sep-2016.

[9] K. Suzuki, "Satellites, the floating targets," *World Today*, no. February & March 2016, 2016.

[10] D. Livingstone, "The Intersection of Space and Cyber Security is a Growing Concern," *Expert Comment*, 25-Nov-2014. [Online]. Available: https://www.chathamhouse.org/expert/comment/intersection-space-and-cyber-security-growing-concern. [Accessed: 09-May-2019].

[11] The National Academies of Sciences, Engineering, and Medicine, "National Security Space Defense and Protection," The National Academies Press, Washington, D.C., Aug. 2016.

[12] D. Fidler, "Cybersecurity and the New Era of Space Activities," 03-Apr-2018. [Online]. Available: https://www.cfr.org/report/cybersecurity-and-new-era-space-activities. [Accessed: 08-Sep-2019].

[13] B. Unal, "Cybersecurity of NATO's Space-based Strategic Assets." Chatham House, Jul-2019.

[14] F. Schreier, "On Cyberwarfare," The Geneva Centre for the Democratic Control of Armed Forces, 2015.

[15] NIAC, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructures," Aug. 2017.

[16] B. Karabacak, S. Ozkan Yildirim, and N. Baykal, "Regulatory approaches for cyber security of critical infrastructures: The case of Turkey," *Computer Law and Security Review*, 2016.

[17] SpaceIGS, "Space Innovation and Growth Strategy, 2014 - 2030 Space Growth Action Plan." UK Space Agency, 01-May-2014.

[18] R. F. Dacey, "Significant Homeland Security Challenges Need to Be Addressed," United States General Accounting Office, Testimony GAO-02-918T, Jul. 2002.

[19] United States, "National Strategy for Homeland Security." Office of Homeland Security, Jul-2002.

[20] United States, "National Security Strategy of the United States of America." The White House, Dec-2017.

[21] Blackhat, "The 2017 Black Hat Europe Attendee Survey: The Cyberthreat in Europe." Blackhat Europe 2017, Nov-2017.

[22] P. B. Stares, “Preventive Priorities Survey 2019.” Council on Foreign Relations, 2019.
[23] J. Molas-Gallart, “Which way to go? Defence technology and the diversity of ‘dual-use’ technology transfer,” *Res. Policy*, vol. 26, no. 3, pp. 367–385, Oct. 1997.
[24] J. Forge, “A note on the definition of ‘dual use,’” *Sci. Eng. Ethics*, vol. 16, no. 1, pp. 111–118, Mar. 2010.
[25] National Research Council, “Biotechnology Research in an Age of Terrorism,” The National Academies Press., Washington, DC, 2004.
[26] J. Molas-Gallart and T. Sinclair, “From technology generation to technology transfer: the concept and reality of the ‘Dual-Use Technology Centres,’” *Technovation*, vol. 19, no. 11, pp. 661–671, Nov. 1999.
[27] J. Johnson-Freese, *Space as a Strategic Asset*. Columbia University Press, 2007.
[28] C. Baylon, “Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives.” Chatham House, Dec-2014.
[29] P. E. Auerswald, L. M. Branscomb, T. M. La Porte, and E. O. Michel-Kerjan, *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, First Edition. New York: Cambridge University Press, 2006.
[30] M. Dunn-Cavelty and M. Suter, “Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection,” *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 4, pp. 179–187, 2009, doi: 10.1016/j.ijcip.2009.08.006.
[31] P. Rosenzweig, “The organization of the United States government and private sector for achieving cyber deterrence,” in *Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC, 2010, pp. 245–279.
[32] J. Stavridis and E. N. Farkas, “The 21st Century Force Multiplier: Public–Private Collaboration,” *Wash. Q.*, vol. 35, no. 2, pp. 7–20, 2012, doi: 10.1080/0163660X.2012.665336.
[33] M. E. Hathaway and A. Klimburg, “Preliminary Considerations: On National Cyber Security,” in *National Cyber Security Framework Manual*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012, pp. 1–43.
[34] A. Klimburg, “The Whole of Nation in Cyberpower,” *Georget. J. Int. Aff.*, pp. 171–179, 2011.
[35] J. A. Lewis, “Aux armes, citoyens: Cyber security and regulation in the United States,” *Telecommun. Policy*, vol. 29, no. 11, pp. 821–830, 2005.
[36] R. J. Harknett and J. A. Stever, “The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen,” *J. Homel. Secur. Emerg. Manag.*, vol. 6, no. 1, pp. 1–14, 2009.
[37] S. J. Shackleford and A. N. Craig, “Beyond the new ‘digital divide’: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity,” *Stanf. J. Int. Law*, vol. 50, no. 1, pp. 119–184, 2014.
[38] Business Software Alliance, “Improving our Nation’s Cybersecurity through the Public - Private Partnership.” 08-Mar-2011.
[39] L. Clinton, “A relationship on the rocks: Industry-government partnership for cyber defense,” *J. Strateg. Secur.*, vol. 4, no. 2, pp. 97–112, 2011.
[40] C. Koski, “Does a partnership need partners? assessing partnerships for critical infrastructure protection,” *Am. Rev. Public Adm.*, vol. 45, no. 3, pp. 327–342, May 2015.

[41] CSIS, “Securing Cyberspace for the 44th Presidency,” Center for Strategic & International Studies, Washington, DC, Dec. 2008.
[42] H. S. Can, G. Ikitemur, and H. M. Hendy, “Measurement of organisational variables associated with cyber security preparedness in Turkey,” *Cyber Secur. Peer-Rev. J.*, vol. 2, no. 2, pp. 181–192, Autumn/Fall 2018.