Journal of Governance, Security & Development
ISSN: 2708-2490
Vol 4 No. 1 2023: Online Early Version
DOI: 10.52823/BOND6012

The Role of Private and Third Sectors in Cybersecurity Governance: The Russian-Ukrainian Cyber Conflict

CAI Cuihong & YU Dahao
Fudan University, People's Republic of China

Abstract:
The private sector and the third sector were once relatively independent actors in global cybersecurity governance. However, with the continuous expansion of the breadth and depth of global security governance and the increasingly fierce geopolitical game, the 'power diffusion' has begun to reverse, and the government has accelerated the 'power collection'. Therefore, the government is now playing a decisive role in global cybersecurity governance. In this context, the role of the private sector and the third sector in global cybersecurity governance has shifted from 'actor' to 'tool'. A case study of private and third sector operations in the Russian-Ukrainian cyber conflict reveals that those two sectors are increasingly taking orders from the government in their home country to participate in cyber security operations at its request, losing their relative independence, which has enormous implications for global cybersecurity governance.

Keywords: Private Sector; Third Sector; Cybersecurity Governance; Russian-Ukrainian Cyber Conflict

Introduction

Since the conflict between Russia and Ukraine began, Europe and the rest of the world have been dealing with one of the most serious security crises since World War II. In addition to the physical conflict, Russia and Ukraine are engaged in large-scale cyber operations in virtual space.

It is worth noting that both the Western and Russian private and third sectors have been deeply involved in Russia's and Ukraine's cyber

offensive and defensive operations under government orders, posing challenges to international law that primarily deals with traditional armed conflicts between sovereign states and reflecting a new trend in cyber security governance.

For example, on 25 February 2022, former United States Secretary of State Hillary Clinton publicly called for hacking groups as a third sector to respond to Russian cyber-attacks (Taihe Institute, 2023). On the same day, the international civil hacker organization, 'Anonymous' announced on its Twitter account that it had launched a 'cyber operation' against Russia in retaliation for Russia's 'invasion' (CNBC, 2022). At the same time, Google, Meta and other Western private sectors also followed the government's ban and shut down Russian accounts on YouTube, Facebook, Instagram and other platforms.

Previously, the government, private and third sectors played relatively independent roles in global cybersecurity governance under the multistakeholder governance model, but this has changed. The cyber conflict between Russia and Ukraine provides a compelling case for investigating the evolving role of cyber security governance actors in the new era. Based on this case, this paper attempts to demonstrate that with the continuous expansion of the breadth and depth of global security governance and the increasingly fierce geopolitical game, the 'power diffusion' has begun to reverse, and the government has accelerated 'power collection'. As a result, the government is now taking a decisive role in global cybersecurity governance. In this context, the private and third sectors' roles in global cybersecurity governance have shifted from 'actor' to 'tool,' causing them to lose autonomy, with significant implications for global cybersecurity governance.

Statement of the Research Questions

Since the birth of the Internet in 1969, human society has witnessed its rapid development (Van Puyvelde & Aaron, 2019: 72). Despite its relatively short history, the Internet has dramatically reshaped contemporary political, economic, and social life (Nye, 2011: 122). People's dependence on the Internet has aroused international community concern for its development, security and stability (DeNardis & Raymond, 2013), and global cybersecurity governance has emerged in many power struggles (Carr, 2015).

In 2005, the Working Group in Internet Governance (WGIG), set up by the World Summit on the Information Society (WSIS), defined Internet governance as: 'development and application by Governments,

the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet' (WSIS, 2005). Among them, civil society is also called the 'third sector', including individual citizens, technical communities, etc., collectively called the 'public sector' with the government. The 'private sector' is a concept opposite to the 'public sector', which can be defined as an industrial and commercial enterprise organization with market regulation as the main body and the purpose of maximizing organizational benefits.

As a vital field of Internet governance, the main actors in global cybersecurity governance are these three. When the concept of Global Governance came into being, its basic meaning was 'Governance without Government' (Rosenau, 1992). The private sector and the third sector are not directly controlled or operated by the government but are usually owned by individuals and teams and are relatively independent actors in global cybersecurity governance.

Due to the emergence, operation mode and endogenous characteristics of cyberspace itself, compared with other global governance areas, the role of the private sector and the third sector is more important in global cybersecurity governance. Understanding the changing role and reality of the private sector and the third sector in global cybersecurity governance is crucial to promoting the establishment of a peaceful, stable and win-win situation in cyberspace to safeguard the virtual and physical security of all humanity in the digital age. Therefore, based on the case of Russia-Ukraine cyber conflict, this paper aims to explore the changing role of the private sector and the third sector in global cyber security governance.

Role of the Private and Third Sectors in Cybersecurity Governance

Madeline Carr (2015) argues that today's cyberspace is mirrored in a struggle for politics, interests, and legitimacy because the Internet has essentially become a projection of government power and a Gramscian cultural hegemony, with the dominant players of the network able to set the agenda and rules by their own power. To some extent, this view reflects a major dilemma of current global cybersecurity governance, that is, the expansion of government power and the behavior of hegemonic countries have extensively interfered with global cybersecurity governance.

In global cybersecurity governance, the private sector once played a

'dominant' role and was a relatively independent actor. The private sector has a huge role to play in regulating cyber content, regulating cyber speech, resolving cyber disputes, and formulating related cyber policies (DeNardis, 2012). Laura DeNardis succinctly describes this role as the privatization of network governance' (Arsene, 2012). In the context of the time, Rebecca MacKinnon bluntly argued that the ubiquity of Google and Facebook in life matched the scope and jurisdiction of the traditional nation-state, making these companies comparable to virtual 'nations' (MacKinnon, 2012). 'Privatization of network governance' is reasonable because the private sector is a virtual 'nation', the scope of sovereignty does not limit its interests, so the private sector as a relatively independent actor from the government, its 'dominant' role in cyberspace is conducive to preventing conflicts between countries in physical space from spreading into cyberspace, thus protecting the security of cyberspace. However, with the development of technology and changes in the real world, the 'dominant' role of the private sector in cybersecurity governance has gradually changed from a relatively independent 'actor' to a 'tool' subordinate to the will of the government.

Looking back in the past, as early as the early days of the Internet, the field of network security governance actually did not have a powerful government role. Even though cyberspace was under U.S. control, it was largely self-regulated, guided by the Department of Commerce and maintained by the technical community (Nye, 2014). In the last century, Internet users mainly came from academic and scientific circles. The number was limited, and all were real names, so the management was relatively straightforward and simple. This initial free governance system is mainly manifested in the private sector and the third sector, which promotes the innovation of network technology, the development of the network economy and the maintenance of network security.

However, soon, with the continuous popularization of the Internet and its penetration into all aspects of society, the existing laissez-faire governance model has become a double-edged sword, which has liberated the vitality of the Internet and brought various problems and risks (Baird & Verhulst, 2004: 1-2). The decentralized nature of the Internet and its interconnection determine the need for a new model of global multi-sector joint governance. The rapid change in Internet ecology has led governments worldwide to realize the urgency of governance model reform at the beginning of the 21st century. At the World Summit on the Information Society (WSIS) in 2005, the participating countries defined cyber governance and established a 'multistakeholder' model with multi-sectoral joint governance. Under this model, governments, the private

sector, and the third sector are co-located in all areas of cyberspace governance.

Regarding the role of the private sector in this model, Laura DeNardis argues that there is a system for maintaining the administrative and technical coordination tasks necessary for the operation of the Internet and the development of related public policies, which range from the development of technical standards and the management of domain names to the development of policies related to cybersecurity and privacy. Most of the tasks in this system can only be performed by the private sector, not by the government (DeNardis & Hackel, 2015). Therefore, the private sector is undoubtedly dominant in this governance system.

In 2012, when Google decided to take steps to block the Innocence of Muslims, a video featuring Muhammad, Peter Spiro declared: 'Google controls the world's information, and the private sector has the power of a sovereign state to decide what stays public and what gets removed' (Musiani, 2012).

Since the establishment of the Westphalian system, sovereign states have been the main actors in the international community. However, Western perceptions shifted in the second half of the 20th century, as the relationship between government, the private sector, and social forces, and their respective roles and functions in the international community, became widely discussed (Carr, 2015). After the end of the Cold War, the U.S. government focused on technology investment, and technological change was regarded as a 'new source of power or resource'. As a direct promoter and user of technology, the status of the private sector was increasingly rising, and it became the dominant player in achieving global economic growth and technological development in the era of advancing globalization.

The reasons for the rise of the private sector can be seen in Sven Bislev and Mikkel Flyverbom's description of the Foucault concept of power, according to which power and resources are equivalent, and whoever has the relevant resources can have influence and power (Bislev & Flyverbom, 2005). Since the second half of the 20th century, the private sector has gained enormous material, technical and human resources.

The innovation and popularization of the new technological revolution enable more individuals to obtain information freely, thus obtaining resources and power, which leads to the emergence of new power types and power subjects. Joseph Nye defines this phenomenon as 'power diffusion,' the diffusion of technological change that facilitates the transfer of power from the state to non-state actors. Nye argues that this form of power transfer will break the monopoly of traditional bureaucracy

and allow non-state actors to play a greater role in world politics. In contrast, state actors will lose control in an increasing number of areas.

In cybersecurity governance, with the 'power diffusion,' the private sector once gained more power. In 2018, as the private sector owned most of the Internet infrastructure, it controlled 90-95% of the Internet's information (Martino, 2018). Therefore, the private sector plays a veritable 'dominant' role in the field of cybersecurity governance. At that point, the relationship between the government and the private sector was a 'partnership' that enabled both parties to reach common agreements and goals.

However, with the continuous emergence of network power and the continuous tension of the geopolitical situation, the 'power diffusion' in global network security governance has gradually stopped, and the government is carrying out 'power collection'. The government is no longer entirely comfortable handing over a large proportion of cybersecurity governance to the private sector and is starting to take over directly itself (Carr, 2015). In fact, the legitimacy of the private sector's role as the dominant player in global cyber governance is inherently flawed. On the one hand, the private sector, which is not elected or selected, represents the interests of a small circle and lacks institutional accountability. On the other hand, the private sector that holds the power of network security governance is basically large technology companies in the United States. If the private sector in emerging markets wants to get a share of the market, it is bound to be suppressed by the United States, so the security governance led by the private sector is facing a great crisis of trust outside the United States.

In response to the growing use of the private sector by governments for national benefit, Madeline Carr has long highlighted the inextricable links between the private sector and the state in cyber governance. She began by tacitly acknowledging that the private sector does play the most direct role in cyber governance, since most Internet infrastructure is owned and operated by the private sector, but that the private sector tends to entrench 'existing world power patterns' in cyberspace (Carr, 2015). Carr's point of view is that the private sector that holds the right to speak is basically multinational corporations headquartered in the United States and closely related to the U.S. government, which makes the current global network governance system more inclined to American values and conducive to the interests of the United States and its Western Allies. In recent years, due to the wave of anti-globalization and increasingly intense geopolitical games, high-tech multinational companies have increasingly deepened their political ties with their home

countries, casting another layer of uncertainty over the private sector's activities in global cybersecurity governance.

In 2013, Edward Snowden revealed that the National Security Agency (NSA), with the help of major private social media platforms such as Facebook, Google, Microsoft and Yahoo, was mining data and gathering intelligence directly into the central servers of U.S. Internet companies. It collected the private information and data of tens of millions of Americans and even spied on many foreign leaders. As a result, many countries, after seeing these large technology companies serving the U.S. government, understand that the highly privatized nature of global cyber governance is a tool for the U.S. to safeguard its own interests and increasingly distrust the private sector, especially the U.S. private sector. The PRISM scandal represents the beginning of a trend in which the private sector can no longer maintain its relative independence in cybersecurity governance and is moving from being an 'actor' to a 'tool' of the government.

Compared with the 'dominant' role played by the private sector in global cybersecurity governance, the third sector, as a relatively independent actor, has played a 'leading and supporting' role. Back when the Internet was born, 'privatization of governance' had not yet occurred, and the presence of governments and the private sector was limited. The original Internet was primarily maintained by the technical community, with a limited number of users, mainly from academia and technology, which was very manageable. This initial liberal network security governance system is mainly manifested as a kind of autonomy led by the third sector. The third sector plays a leading role in the early stages.

Soon, with the increasing complexity of cybersecurity governance, the U.S. government began the process of commercialization and privatization of infrastructure in the Internet field, entrusted the management and operation of critical infrastructure to the U.S. private sector, promoted local companies to control the global Internet industry chain, and further transferred the power and responsibility of the public sector to the private sector. The third sector shifted into a 'supporting' role, providing technical and managerial support to the private sector.

One of the most telling examples is the work of the Internet Engineering Task Force (IETF), which is a large public civil society, founded at the end of 1985. It is the world's most authoritative technical standardization organization whose main task is to be responsible for developing and formulating Internet-related technical specifications. At present, the vast majority of international Internet technical standards come from IETF, which brings together network designers, operators and

researchers related to the evolution of Internet architecture and the stable operation of the Internet and is open to all those who are interested in the industry. It can be said that it is the most important third sector in the global Internet governance system and an essential part of the relevant public sector. However, with the advent of the era of great change, like the private sector, today's third sector is also gradually shifting from a relatively independent 'actor' in a 'multistakeholder' model to a 'tool' of government.

Private and Third Sectors in the Russian-Ukrainian Cyber Conflict

A case study of private sector and third sector operations in the Russian-Ukrainian cyber conflict reveals the fact that those two sectors are increasingly taking orders from government in their home country to participate in cyber security operations at its request, losing their relative independence, which has huge implications for global cybersecurity governance. In this conflict, the third sector first showed signs of changing from 'actor' to 'tool'.

As early as the 2014 Crimean crisis, hackers with ties to Russian intelligence services have launched cyberattacks on Ukraine at the behest of the government (Europa, 2022). Their targets include government agencies, universities, power companies, the banking sector and other critical infrastructure. At the time, Russia's goal was to antagonize the Ukrainian public and weaken Russia's political opponents in the Ukrainian political system. In some cases, the attack authors deployed malware that had never been used before, making Ukraine a testing ground for new types of cyberweapons. Starting in 2014, the Pro-Russian hacker group CyberBerkut installed malware in Ukraine's central election system to leak secrets, thereby undermining public trust in the electoral process and causing political instability. CyberBerkut reportedly has close ties with the General Staff Intelligence Directorate of the Russian Federation (GRU). In addition, on election day, CyberBerkut launched a massive Distributed Denial-of-Service (DDoS) attack campaign to delay the final election count and discredit the election process in the eyes of the public.

However, the attack failed in delegitimizing the election winner. Ukrainian cybersecurity personnel removed the malware from the system in time to prevent it from posting fake election results, but the final tally was delayed by two hours (CCDCOE, 2014). In 2015, Sandworm, an advanced persistent threat group linked to the GRU, successfully

launched a cyber-attack on Ukraine's power grid and publicly acknowledged it for the first time. The attackers successfully took remote control of the data acquisition and surveillance control systems of three Ukrainian energy distribution companies. They knocked out power in three provinces in western Ukraine, leaving about 225,000 people without electricity for up to six hours (CCDCOE, 2015). In 2016, nearly a year after the last attack, the Ukrainian energy grid was again targeted. The attackers deployed the Industroyer malware, which became the biggest threat to industrial control systems since Stuxnet. This malware is used to control substation switches and circuit breakers remotely. It is achieved by installing backdoors into the target system exploiting vulnerabilities in the Industrial Control Systems (ICS) protocol throughout the critical infrastructure. The cyber-attack, which affected a large part of the Ukrainian capital, is believed to be the work of the Advanced Persistent Threat Group Electrum, directly linked to Sandworm (CCDCOE, 2016). The most serious cyber incident in Ukraine occurred in 2017, when the destructive NotPetya malware was deployed against Ukraine's financial and energy sectors by Telebots, a Russian advanced persistent threat organization also linked to the Sandworm. NotPetya was named for its similarity to ransomware Petya, which attacked in early 2016 and blackmailed victims without providing them with the key to unlock files. This time, regardless of whether the victims paid the extortionists, NotPetya compromised 10 percent of computers in Ukraine, rendering them unable to boot. It spread throughout Ukraine's financial sector through a popular tax preparation procedure. Although the attack targeted companies in Ukraine, the malware spun out of control and affected several multinational companies in Europe and the United States. The exact impact on Ukraine's economy is not yet known but estimates of global economic losses exceed $10 billion (CCDCOE, 2017).

It is not only the pro-Russian third sector that conducts cyber operations at the government's behest but also the pro-Ukrainian third sector that frequently launches attacks. Shortly after Moscow launched military operations against Ukraine in February 2022, Anonymous, as the third sector of the civil hacker organization, responded to the call of former U.S. Secretary of State Hillary Clinton and tweeted that it would gather international forces to launch cyber warfare against Russia because it invaded Ukraine (Lin, 2022). The targets included Russian government agencies, state-run television channels and the central bank, and the group went on to publish 230,000 leaked emails from a Russian city government, as well as 28 gigabytes of data obtained from the Central

Bank of Russia. Meanwhile, Killnet, a Russian private hacking group, announced that it had destroyed the website of the Anonymous hacking group that attacked Russian Internet resources and called on Russians 'not to be influenced by false information on the Internet and not to doubt their country under any pretext' (Incyber Forum, 2022).

On 2 March 2022, the Russian government published a list showing that more than 17,500 IP addresses and 174 Internet domains were involved in ongoing DDoS attacks against targets in Russia, including government agencies such as the FBI and the CIA, as well as several hacker groups registered in Ukraine and the European Union. The official website of the Russian Federal Savings Bank (Sberbank) revealed that on 6 May 2022, it successfully repelled the largest ever DDoS attack, with the attack traffic coming from 27,000 private hacker organizations in the United States, the United Kingdom and Japan.

In a speech in Tallinn in June 2022, Paul Nakasone, commander of U.S. Cyber Command and director of the National Security Agency, acknowledged that the U.S. military was conducting a 'full range' of offensive, defensive and information operations against Russia. He also revealed that U.S. Cyber Command experts have been deployed to 16 countries in the U.S. alliance to assist allies in obtaining intelligence from relevant organizations and working together (Martin, 2022).

The Russian government usually underplays incidents of civilian hacking, partly to avoid damaging Russian military morale and partly to avoid disputes with Western governments. The West, in turn, shirked its own government's responsibility, accusing the Russian government of colluding with civilian hackers. Under the government's command, the network action that the third sector participates in is not only the attack and defense of network security but also the struggle of international law and international public opinion.

While the third sector is engaged in cyber conflict, the private sector is also acting as a tool of geo-warfare at the behest of governments. The West has taken advantage of its private sector's advantages in digital technology and discourse power to block Russia's voice channels completely. The United States, Australia, Spain, France, Germany, Canada, the United Kingdom and other Western countries have asked their relevant private sectors to block Russian media and accounts.

Ukraine's success so far in defending itself against Russian cyberattacks has been mainly due to the involvement of the private sector at the behest of the U.S. government. The U.S. private sector, including Microsoft, Amazon and SpaceX, has provided Ukraine with commercial solutions such as digital cloud services and Starlink, as well as critical

communications infrastructure to help Ukraine gain an advantage in the Russian-Ukrainian cyber conflict.

In the Russia-Ukraine cyber conflict, at the government's request, the participation of the private sector takes various forms, compared with the participation of the third sector, which is a relatively single hacker organization.

From commercial satellites to drones, mobile phone apps to social media, Western tech giants and even start-ups not only help Ukraine keep its networks running smoothly but also help Kiev gather intelligence and fight information and psychological warfare. The combination of emerging technologies and traditional weapons, as well as the war of opinion, has tipped the balance of power on both sides of the conflict.

First, the private sector operates behind the scenes, participating in cyber-attacks and defenses. Long before the outbreak of the conflict between Russia and Ukraine, Western technology companies were working at the request of the government to strengthen Ukraine's cyber defenses and ensure the stability and smooth flow of the Internet in Ukraine. Nakasone said U.S. government experts had traveled to Ukraine months before the conflict began. Microsoft and Google have worked with Ukraine even earlier. In many cases, it was Western tech companies that took the lead in securing all aspects of Ukraine's Internet at the request of the government, without the direct involvement of Ukrainian and Western governments. The backbone of the Internet -- the wires, servers and the like that keep it running -- is fragile, and several Western companies, such as SpaceX, have played a crucial role in maintaining Ukraine's backbone. After the conflict broke out, SpaceX CEO Elon Reeve Musk quickly responded to a request from the Ukrainian government to provide Internet connectivity to Ukraine. Microsoft provides network licenses and services to Ukrainian institutions to move critical Ukrainian software services to the cloud to ensure their continuity. These operations allow Ukraine to smoothly conduct daily data transfers and help fighters obtain intelligence data.

Nakasone confirmed that Microsoft's Threat Intelligence Center played an important role in detecting and resolving the cyberattack against Ukraine. Microsoft claims that Russia launched nearly 40 attacks between 23 February and 8 April 2022 alone, but Ukraine worked with Western private tech companies and intelligence agencies to quickly repair most of the damage (Microsoft, 2022). A Microsoft executive said the company had provided financial and technical assistance worth hundreds of millions of dollars to Ukraine. Google has expanded its ‘Project Shield’ to protect more than 150 Ukrainian political

organizations, as well as press and publishing organizations. In addition, Amazon also put some of the Ukrainian agency's Web services on the Amazon cloud to protect them from attacks. Other private sector moves to cut Russia off from the global Internet at the request of the government. For example, Cogent Communications and Lumen Technologies decided to stop providing Internet backbone services to Moscow. This has left Russia's major telecom operators, such as Trans telecom (TTK), having to find other ways to carry their Internet traffic, further affecting Moscow's communications and intelligence acquisition capabilities in the conflict. Second, the private sector is conducting a digital blockade against Russia in cyberspace. When the shells of Russia and Ukraine rained down on each other's entrenchments, another 'war' was breaking out in cyberspace, and the 'war' in addition to the two sides, there were Western social media platforms such as Twitter, Facebook, Google, Microsoft and other technology companies. After Western countries announced a series of tough sanctions against Russia, some Internet technology companies followed suit with restrictions -- Google announced that its video site YouTube had banned the accounts of Russia Today (RT) and Sputnik from Posting to Europe; Meta introduced similar measures to 'YouTube'; Twitter tagged posts whose sources are linked to the Kremlin. In addition, Microsoft no longer shows RT and Sputnik products and ads and has removed RT-related apps from its app store.

Indeed, Western Internet companies are already at the mercy of Western governments in the online public opinion war, doing everything they can to help Ukraine. Previously, posting content on Facebook that praised neo-Nazi militias or called for violence against Russians could get you banned. Now, in the context of the conflict between Russia and Ukraine, the publication of such content has been tacitly tolerated. At the same time, Russian state media accounts, which once enjoyed 'freedom of speech,' are blocked in Europe. These initiatives show a shift in the principle of political neutrality that the private sector is supposed to embrace. Social media has long been a place where information is gathered and shared and where true and false information is disseminated. In the Russian-Ukrainian cyber conflict, the pro-Ukrainian side has helped Kiev project the image of a 'strong survivor' by displaying a large number of photos of war casualties while portraying Russia as a 'ruthless aggressor' and condemning Moscow. In response, Russia has stepped up its campaign against Western Internet companies. On 11 October 2022, Russia's Financial Services Agency added Facebook's parent company Meta to its list of terrorist and extremist organizations (Euronews, 2022).

The performance of the western private sector in the Russia-Ukraine conflict shows that the 'politicization' of the private sector in cybersecurity governance is deepening. Western military companies have long played an important role in regional wars, such as building tanks, aircraft and weapons, but they are not often involved in battlefield operations, and now some Western technology companies have become participants in the conflict.

The involvement of the private sector in cyberspace conflicts, directly mandated by governments as their 'tools', has brought about a completely new picture of global cyberspace governance.

Conclusion

At the moment, the cyber conflict between Russia and Ukraine is a contest between many national and regional governments, the private sector, and the third sector, and even the US government directly promotes the deployment, mobilizes the private sector and the third sector, and continues to pressure and sanction the Russian side. The participation of numerous forces will collectively heighten the network confrontation in the Russian-Ukrainian conflict.

The Russia-Ukraine cyber conflict provides a clear example of the changing roles of the private sector and the third sector in global cyber security governance, that is, in the new era, with the continuous expansion of global cyber security governance in breadth and depth and the increasingly fierce geopolitical game, the private sector and the third sector in global cyber security governance have changed from relatively independent 'actors' to 'tools' of the government, and the government has become the absolute dominant force in the field of cyber security governance.

In this Russian-Ukrainian cyber conflict, the private and third sectors have lost their neutrality. They can no longer make unbiased value judgments about how governments utilize their platforms during wartime or determine which types of speech violate regulations. Consequently, their ability to independently govern has been compromised. This situation has far-reaching implications, not only for the course of cyber conflict, but also for the future of cyber governance. The participation of different private sectors and third sectors in the cyber conflict between Russia and Ukraine indicates that in future cyber security conflicts, the dynamics between nations will present a complex struggle situation under governmental guidance. This battle will not only be fought by governments, but also by private companies and the third sector. In the

future, it is expected that the private and third sectors will increasingly become tools of governments rather than independent actors. This shift will further exacerbate the global cybersecurity governance deficit.

References

Arsene, S. (2012). The impact of China on global internet governance in an era of privatized control. Chinese Internet Research Conference, Los Angeles.

Baird, Z. & Verhulst, S. (2004). *A New Model for Global Internet Governance*. New York: United Nations ICT Task Force.

Bislev, S. & Flyverbom, M. (2005). Global Internet Governance: What Roles do Business Play? ECPR (European Consortium for Political Research) Joint Sessions, April 14-19, 2005. https://ecpr.eu/Filestore/PaperProposal/dba8c7a7-58e5-4ea7-9ec1-2a2ddc939baa.pdf. Accessed 17 October 2023

Carr, M. (2015). Power plays in global internet governance. *Journal of International Studies,* 43(2): 455-659.

CCDCOE (2014). Ukrainian parliamentary election interference (2014). https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014). Accessed 27 October 2023.

CCDCOE (2015). Power grid cyberattack in Ukraine. https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015). Accessed 27 October 2023.

CCDCOE (2016). Industroyer – Crash Override (2016). https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_(2016). Accessed 27 October 2023.

CCDCOE (2017). NotPetya. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017). Accessed 27 October 2023.

CNBC (2022). Global hacking group Anonymous launches cyber war against Russia. https://www.cnbc.com/2022/03/01/how-is-anonymous-attacking-russia-disabling-and-hacking-websites-.html. Accessed 18 December 2023.

DeNardis, L. & Raymond, M. (2013). Thinking clearly about multistakeholder internet governance. The 8th Annual GigaNet Symposium, 21 October 2013.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377. Accessed 18 December 2023.

DeNardis, L. & Hackel, A. (2015). Internet Governance by social media platforms. *Telecommunications Policy*, 39(9): 761-770.

DeNardis, L. &Musiani, F. (2016). *The turn to infrastructure for internet governance: Governance by Infrastructure*. New York: Palgrave Macmillan.

Euronews (2022). Russia adds Meta to list of 'terrorist and extremist organizations'. https://www.euronews.com/2022/10/12/russia-adds-meta-to-list-of-terrorist-and-extremist-organisations. Accessed 17 November 2023.

Europa (2022). Russia's war on Ukraine: Timeline of cyber-attacks,2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.Accessed October 21, 2023.

Incyber Forum (2023). Anonymous declares war on Russian Killnet hackers. https://incyber.org/en/anonymous-declares-war-on-russian-killnet-hackers/. Accessed 27 October 2023.

Lin, H. (2022). Russian Cyber Operations in the Invasion of Ukraine. *The Cyber Defense Review*, 7(4): 31-46.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for internet Freedom*. New York: Basic Books.

Martin, A. (2022). U.S. military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139. Accessed 17 October 2023.

Martino, L. (2018). La quinta dimensione della conflittualità, lascesa del cyberspazio ei suoi effetti sulla politica internazionale. *Politica & Società*, **1**: 61-76.

Microsoft (2022). An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. Accessed 17 November 2023.

Musiani, F. (2012). Google and Video Blocking: Control (and Responsibility) of Information Intermediaries on the Internet. http://adam.hypotheses.org/1383. Accessed 7 December 2023.

Nye, J. (2011). *The Future of Power*, New York: United States Public Affairs.

Nye, J. (2014). The regime complex for managing global cyber activities. Chatham House, Paper series No. 1. https://www.cigionline. org/sites/ default/files/gcig_paper_no1.pdf. Accessed 18 December 2023.

Rosenau, J. (1992). *Order and Change in World Politics*. Cambridge: Cambridge University Press.

Taihe Institute (2023). How the U.S. Exports Democracy and Endangers the World. http://www.taiheglobal.org/Content/2023/09-08/1736000255.html. Accessed 30 November 2023.

Van Puyvelde, D. & Aaron, B. (2019). *Cybersecurity Politics, Governance and Conflict in Cyberspace*. Cambridge: Polity Press.

WSIS (2005). Agenda for the Information Society. https://www.itu.int/net/wsis/outcome/booklet/tunis-agenda_C.html. Accessed 2 December 2023.

About the Authors

CAI Cuihong PhD is a professor of international relations at the Center for American Studies at Fudan University, People's Republic of China. She received her doctorate in international relations from Fudan University in 2002. She was a visiting scholar at the Georgia Institute of Technology, the University of California, Berkeley, as well as an invited fellow in the program on the U.S. National Security sponsored by the U.S. State Department. Dr. Cai is the author of *Global Governance of Cyberspace* (2023), *Cyberpolitics in U.S.-China Relations* (English version 2021, Chinese version 2019), *Political Development in the Cyber Age* (2015), *U.S. National Information Security Strategy* (2009) and *Internet and International Politics* (2003). She is an expert on cyberpolitics, cybersecurity strategy, cyberspace governance, and U.S.-China relations.

YU Dahao is a PhD candidate in international political economy at the School of International Relations and Public Affairs of Fudan University. He holds a master's degree in international relations from Fudan University, and has visited and studied in the European Union, Australia, South Korea, and participated in the work of the United Nations. His research interests include global digital governance, international digital economy and cyberspace security.