ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

# Introduction to Special Issue on

## The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure

**Jacek Leśkow** | American University Kyiv Ukraine |
ORCID: 0000-0003-2228-393X

**Received:** 12.02.2024

**Accepted:** 24.05.2024

**Published:** 23.07.2024

**Cite this article as:**
J. Leśkow "Introduction to Special Issue on The Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure" ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/191475

**Corresponding author:**
Jacek Leśkow, Rector, American University Kyiv Ukraine. E-Mail: xyz@abc.com;
0000-0003-2228-393X



Dear Readers,

I am pleased to introduce a special edition of *Applied Cybersecurity & Internet Governance* (ACIG) journal dedicated to the Russian-Ukrainian war and the associated cybersecurity risks. The conflict started by Russia in 2014 with illegal annexation of Crimea and a part of Donbas region has a profound implication. Our civilisation shifts to the digital dimension; therefore, understanding cybersecurity within this context has become more critical than ever.

I would like to invite readers to reflect on some key questions: How did the Russian-Ukrainian war emerge after a prolonged period of peace? What political processes lead to the loss of tens of thousands of Ukrainian lives, the displacement of hundreds of thousands in Ukraine, and the migration of millions of Ukrainians seeking refuge in the European Union (EU) and North America? The answer is, however, that it is essential to identify crucial factors contributing to the current crisis, also in cyberspace. The first fundamental factor is the lack of strong moral condemnation of the Soviet system based on communist ideology. Unlike luminaries of fascist regimes, communist perpetrators were never held accountable for their horrible crimes committed in the 20th century. Historical research proves that Stalin and his followers were responsible for the deaths of at least three times more innocent civilians than Nazis. While Nazi German concentration camps are presented as historical sites, Soviet *gulags* are not memorised similarly. Some Western

intellectuals have even supported Soviet-style communism. For instance, a major plaza in Naples, Italy, was named after Togliatti, an Italian-born communist and a strong supporter of Stalin.

After the collapse of the Soviet system, many Western countries did not insist on moral accountability for crimes committed by communists. Instead, Western elites moved to the 'business as usual' approach that resulted in two fundamental flaws of Western policy with respect to Russia. These two biggest flaws being the reset policy with Russia originated by US elites and the Nord Stream gas pipeline, a Russian-German cooperation. Both reset policy and Nord Stream initiatives were strongly supported by decision circles of the West after Putin attacked Chechnya, brutally killing tens of thousands of innocent civilians. No change in reset or Nord Stream was done after Putin's Russia attacked Georgia, annexing 10% of its territory. Therefore, in the criminal mentality of Putin and his aides, such an approach of the West was understood as condoning every crime of Russia as long as cheap gas flows in and hundreds of millions of euros per day flow to Russian accounts.

This policy enabled Russia to rebuild its military strength with financial gains from gas exports to Western Europe, facilitating a resurgence of Russian imperialism with the consistent support of Western political elites.

Another fundamental factor in the Russian-Ukrainian war is the Ukraine's aspiration for independence and alignment with the EU. Since the early 2000s, I have frequently visited major Ukrainian universities, such as Kyiv, Dnipro, Odesa, and Lviv. The first significant shift from the communist past occurred during the Orange Revolution in 2004. Although Ukraine then was still divided, with the West being pro-European and the East more pro-Russian, democratisation had begun, and the Stalinist past has been criticised widely. Symbols of communism, such as the statues of Lenin, were finally removed, and new West-oriented political and economic elites have emerged. In my frequent meetings with Ukrainian academics and business people I was asked the question regarding the successes of democratisation in Poland. I realised then that my home country, Poland, was an example to follow for Ukraine. The second, even more significant breakthrough in recent Ukrainian history was the Revolution of Dignity in 2014. Ukraine then has turned out to be more unified in the desire of being pro-European.

So, in recent decade we have seen two conflicting trends. The growth of the totalitarian regime in Russia was financially

supported by Western political elites and the strong pro-independence, anti-totalitarian attitudes of Ukrainian elites. The sheer existence of democratic Ukraine, where many among political elites were first-language Russians (President Volodymyr Zelensky being the most prominent example), was an existential threat to imperialist Russia run by criminals such as Vladimir Putin and his closest aides. That is why Ukraine is such an existential danger to Putin's regime, and that is why Putin is using the potential of the Russian army to destroy Ukraine.

Understanding these historical and political circumstances is essential for comprehending the cybersecurity risks associated with the ongoing conflict. This edition of the ACIG aims to explore these risks in depth, providing valuable insights into the complex interplay between geopolitics and cybersecurity.

Putin's Russia, being the biggest terrorist organisation on our planet, represents a significant threat to global security, employing various means to disrupt the vital processes of numerous democratic countries. This capability is used deliberately and systematically to destabilise the digital value chains of our modern civilisation. Numerous cyberattacks on transportation or communication infrastructure have been attributed to Russian state- and non-state-sponsored actors. In response to these challenges, we remain united and resilient, with a firm belief in our ability to overcome hostile actions.

One crucial strategy to ensure our success is to conduct continuous research on the cyber threats posed by anti-democratic states. This objective motivated the preparation of this special volume of research articles dedicated to the Russian-Ukrainian war and its impact on cybersecurity.

In this volume, there are a total of 12 articles. The special issue opens with the article 'Russia's cyber campaigns and the Ukraine War: From the "gray zone" to the "red zone"'. The author clearly identifies the importance of the fifth battlefield – cyberspace combined with the traditional four dimensions: land, air, sea, and space. The author emphasises the danger of a hybrid war fought with all available means by the Russians. The importance of information warfare as an element of hybrid war is also emphasised in the second article, 'Moscow and the world: From Soviet active measures to Russian information warfare'. The author shows the key importance of information warfare used by Putin's Russia in

waging the kinetic war with Ukraine and the cyberwar with democratic countries. It is, nevertheless, clear that the start of a full-scale war between Russia and Ukraine had an immense impact on global politics. How the so-called pariah states cooperate with China is a topic of our third article entitled, 'Collaborating pariahs: Does the Ukraine War cement and adversarial cyber-information bloc?' In our volume, the global aspects of the Russian-Ukrainian war are also accompanied with more specific discussions on information war and the so-called 'cognitive hacking'. The fourth article of our volume is dedicated to a precise description of this process. One of the countries that is highly digital and, at the same time, highly prone to possible Russian cyber or kinetic attacks is Estonia. The role of Estonia in providing Ukraine significant expertise in cyber defence is a topic of the fifth article of this special volume. Rest of the articles, that is sixth to tenth, in our volume are dedicated to more technical aspects of cybersecurity, such as digital tools of battlefield situational awareness, support of the EU for Ukraine cyber defence, or quantitative risk-based approach of network cyber defence. All articles in this special volume cover a wide range of topics pertinent to current political processes influenced by the Russian-Ukrainian conflict. We aim to contribute significantly to the understanding of political processes that are now stimulated by the Russian-Ukrainian conflict. The Editorial Board and I agree that democracy is currently facing its most substantial challenge after the end of World War II. It is imperative to enhance our understanding of the situation and the digital tools that adversaries used against democracies. Ukraine is enduring significant losses, including population displacement, infrastructure destruction, and paralysing cyberattacks. Despite these challenges, we believe that democracy will prevail, and the reconstruction of Ukraine will commence. This conflict has also strengthened cooperation among democratic countries, underscoring that unity and mutual support are crucial for overcoming contemporary military threats.