NASK©

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE ISSN 2956-3119

2024, Vol. 3, No. 1

SPECIAL ISSUE ON THE RUSSIAN-UKRAINIAN WAR: EFFECTS ON GLOBAL CYBERSECURITY AND DIGITAL INFRASTRUCTURE GUEST EDITOR: JACEK LEŚKOW

Jacek Leśkow
Introduction to Special Issue on the Russian-Ukrainian War: Effects on Global Cybersecurity and Digital Infrastructure
https://www.acigjournal.com/Introduction-to-Special-Issue-on-The-Russian-Ukrainian-War-Effects-on-Global-Cybersecurity,191475,0,2.html

What are the cybersecurity implications of the Russian-Ukrainian war, and how do they affect global digital infrastructure? Prof. Jacek Leśkow introduces a special issue of ACIG, featuring a collection of articles that offer a comprehensive analysis of the geopolitical and technical aspects of cybersecurity within the context of the Russian-Ukrainian war. This issue provides critical insights for researchers, policymakers, and cybersecurity professionals, bridging the gap between global events and their impact on the digital domain.

Roger Kanet
Moscow and the World: From Soviet Active Measures to Russian Information Warfare
https://www.acigjournal.com/Moscow-and-the-World-From-Soviet-Active-Measures-to-Russian-Information-Warfare,187619,0,2.html

What lessons can we draw from the evolution of Russian information warfare from Soviet active measures to today's disinformation campaigns? Russia under Vladimir Putin has revitalized and expanded upon the USSR's tactics of propaganda and disinformation. The Soviet Union primarily targeted foreign elites and decision-makers; however, modern Russia casts a wider net. It aims to influence mass audiences worldwide, particularly through digital platforms to destabilize geopolitical adversaries and bolster its global influence.

Kristan Stoddart
Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'
https://www.acigjournal.com/Russia-s-Cyber-Campaigns-and-the-Ukraine-War-From-the-Gray-Zone-to-the-Red-Zone-,189358,0,2.html

How did Russia's cyber campaigns impact the course of its invasion of Ukraine? Russia's cyber operations, from targeting energy grids to communication networks, were integral to its broader military strategy, yet ultimately fell short due to Ukraine's preparedness and international support. Kristan Stoddart investigates how Ukraine's strengthened cyber defenses disrupted Russia's plans for a swift victory, revealing that key infrastructure protection helped prevent major disruptions.

Chris Bronk
Collaborating Pariahs: Does the Ukraine War Cement an Adversarial Cyber-Information Bloc?
https://www.acigjournal.com/Collaborating-Pariahs-Does-the-Ukraine-War-Cement-an-Adversarial-Cyber-Information,190263,0,2.html

How does the Ukraine war shape the dynamics between pariah states in the realm of cyber and information warfare? Chris Bronk investigates the increasingly coordinated efforts of Russia, Iran, North Korea, and China in response to the Ukraine conflict, creating an informal adversarial bloc against Western influence. The study examines how these states are not only advancing their cyber capabilities but also aligning their information operations to undermine global stability.

NASK©

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE ISSN 2956-3119

2024, Vol. 3, No. 1

SPECIAL ISSUE ON THE RUSSIAN-UKRAINIAN WAR: EFFECTS ON GLOBAL CYBERSECURITY AND DIGITAL INFRASTRUCTURE
GUEST EDITOR: JACEK LEŚKOW

Matthew Crandall
Understanding Estonia's Cyber Support for Ukraine: Building Resilience, Not Status
https://www.acigjournal.com/Understanding-Estonia-s-Cyber-Support-for-Ukraine-Building-Resilience-Not-Status,190396,0,2.html

How did Estonia contribute to Ukraine's cyber defense during the war with Russia? Estonia, known for its cyber expertise, provided substantial cyber support to Ukraine, focusing on practical assistance rather than seeking international recognition. Estonia played a key role in safeguarding Ukrainian digital infrastructure by helping relocate critical systems to NATO territories, facilitating cloud migrations and creating the Tallinn Mechanism, which systematizes cyber assistance to Ukraine.

Viktor Putrenko, Nataliia Pashynska
Military Situation Awareness: Ukrainian Experience
https://www.acigjournal.com/Military-Situation-Awareness-Ukrainian-Experience,190341,0,2.html

How has the Ukrainian military transformed its approach to situational awareness during the ongoing conflict? The authors investigate Ukraine's rapid advancement in military information systems, highlighting how situational awareness (SA) tools have evolved amidst the war with Russia. With a focus on cutting-edge technologies like the Delta system and volunteer-driven innovations, this study offers an in-depth analysis of how these tools are reshaping modern warfare.

Alina Bârgăoanu, Mihaela Pană
Cyber Influence Defense: Applying the DISARM Framework to a Cognitive Hacking Case from the Romanian Digital Space
https://www.acigjournal.com/Cyber-Influence-Defense-Applying-the-DISARM-Framework-to-a-Cognitive-Hacking-Case,190196,0,2.html

How can cognitive hacking influence an entire population? The authors present a case study from Romania of how seemingly harmless YouTube ads can be part of a sophisticated cognitive hacking campaign. Using the DISARM framework, they uncover the strategies behind these cyber influence operations and offer insights into how they can be detected and countered.

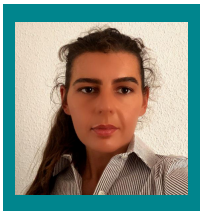
NASK©

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE ISSN 2956-3119

2024, Vol. 3, No. 1

SPECIAL ISSUE ON THE RUSSIAN-UKRAINIAN WAR: EFFECTS ON GLOBAL CYBERSECURITY AND DIGITAL INFRASTRUCTURE GUEST EDITOR: JACEK LEŚKOW



Marina Miron, Rod Thornton

The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?

https://www.acigjournal.com/The-Use-of-Cyber-Tools-by-the-Russian-Military-Lessons-from-the-War-against-Ukraine,190142,0,2.html

How has Russia used cyber tools as part of its military strategy during the war in Ukraine and what does this mean for NATO? The authors analyze Russia's dual approach in cyber operations: cyber-psychological tactics to manipulate public opinion and cyber-technical attacks targeting critical infrastructure. Highlighting operations like the Sandworm group's power grid attacks in Ukraine, the study explores how these strategies create strategic disruption. It also raises concerns that Russia may be reserving its most potent cyber capabilities for a potential future conflict with NATO.

Anna Szczepańska-Przekota

Assessment of the Cybersecurity of Ukrainian Public Companies Listed on the Warsaw Stock Exchange S.A.

https://www.acigjournal.com/Assessment-of-the-Cybersecurity-of-Ukrainian-Public-Companies-Listed-on-the-Warsaw,190343,0,2.html

How do cyberattacks impact the financial stability of Ukrainian companies listed on the Warsaw Stock Exchange? Prior to 2022, cyberattacks had minimal impact on stock values. However, the onset of the Russia-Ukraine war drastically increased market volatility and led to significant declines in the value of the Ukrainian company stock index following cyber incidents. The paper proves the growing sensitivity of financial markets to cybersecurity risks in politically unstable regions and calls for robust cybersecurity measures among publicly traded companies.

Grzegorz Przekota

Investment in Cybersecurity Companies in Times of Political and Economic Instability

https://www.acigjournal.com/Investment-in-Cybersecurity-Companies-in-Times-of-Political-and-Economic-Instability,190342,0,2.html

Is investing in cybersecurity companies during times of political and economic instability a profitable strategy? The COVID-19 pandemic and the Russia-Ukraine war have impacted the financial performance of cybersecurity firms. While some companies, such as Palo Alto Networks and Fortinet, achieved above-average returns, others did not perform as well. Not every tech company benefits from crises, which proves the need for a critical assessment of potential investments in the cybersecurity sector.

NASK©

ACIG

APPLIED CYBERSECURITY & INTERNET GOVERNANCE ISSN 2956-3119

2024, Vol. 3, No. 1

SPECIAL ISSUE ON THE RUSSIAN-UKRAINIAN WAR: EFFECTS ON GLOBAL CYBERSECURITY AND DIGITAL INFRASTRUCTURE
GUEST EDITOR: JACEK LEŚKOW