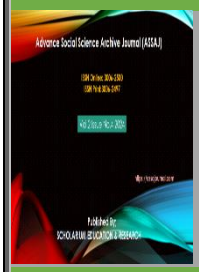

Advance Social Science Archives Journal
Available Online: https://assajournal.com
Vol.3 No.1,January-March,2025.Page No.373-385
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

THE NOTPETYA CYBER-ATTACK: RUSSIA-UKRAINE CONFLICT AND ITS IMPACT ON THE REGIONAL ECONOMIES

Sana Hassam | MS Scholar at Department of Political Science and International Relations - University of Management and Technology, Lahore

ABSTRACT

In 2017, the NotPetya attack, widely cited as Russian-sponsored cyber-attacks against Ukraine, marked the dawning of the future of cyber war as a means of statecraft, with implications for local economies and global politics. This paper draws on realist theory to analyze the geopolitical implications of the NotPetya attack against Russia and Ukraine through power relations, state sovereignty and security problems. In overturning Ukrainian infrastructure and economic structures, the attack showed just how cyber operations can extend age-old power struggle into the digital realm. This spillover to the local economies, as well as collateral damage to international companies and neighboring states, reminds us how cyber threats are global in nature. It shows that current international arrangements have failed in combating state-sponsored cyber-attacks, and demands a revision of security paradigms to stop such attacks. The discussion informs a more general discussion about cyber warfare, its use in state strategies, and its impacts on regional stability and economic resilience.

Keywords: NotPetya cyber-attack, Russia-Ukraine war, regional economies, cyber war, realist theory.

Introduction

The NotPetya cyber-attack in 2017 was one of the most significant attacks in the history of cyber warfare, and its impact was across boundaries, sectors and business lines. It originated in Ukraine, but the malware quickly swept around the world and disabled multinational companies, critical infrastructure and governments alike. This hack – widely blamed on the Russian government – was a prime example of cyber as a means of influence and force in the new international order. To IR realists, the NotPetya incident shows how state interests, power dynamics and the anarchy of cyberspace as a theatre of warfare play out. It was not only that the attack evinced the

dangers of networks, it also emphasized the strategic importance of cyberspace in modern geopolitics 1

Behind this phenomenon, there is also the current geopolitical battle between Russia and Ukraine. In the wake of Crimea's annexation in 2014 and the war in eastern Ukraine that followed, Russia has used mixed warfare, including cyber warfare, to break Ukraine and claim its territory. The NotPetya attack was an important part of this plan, which was meant to halt Ukraine's economy, dent its people's faith in its government, and destroy its sovereignty. The attack at the same time communicated Moscow's strength and determination to local and international spectators. By going after important infrastructure and private organizations,2 Russia demonstrated it was not afraid to deploy cyber capabilities in pursuit of its objectives. Ukraine's response – constrained by its lack of resources and ongoing internal troubles – is a measure of its dependency on outside aid and attempts to control the power imbalance that exists in its conflict with Russia. However, these limitations do not deter Ukraine's growing partnership with its Western partners in cyber defense as it demonstrates that it is ready to create defenses against them.

US, which has a stake in global cyber security and is Ukraine's strategic partner, had a major indirect effect of the attack. NotPetya revealed faults in key US infrastructure and private sector systems – global shipping, logistics, and pharma markets were all compromised. These accumulating impacts forced an evaluation of US cyber defense postures and brought to the fore the nexus of cyber risk. Washington's official position – Russian being the top cyber adversary – has since been underwritten by sanctions, diplomacy and increased cyber investments. This response by the US government has involved measures to build public-private partnerships, sharing threat intelligence and deterring adversaries with both offensive and defensive cyber. All of this follows from the realist focus on power balancing and deterrence against threats, which is how states seek to secure their positions in an anarchic international order.

Further, the NotPetya incident revealed the lapses in existing international standards and laws in the resolution of cyber-conflicts. Since there are no proven fault lines or punishable consequences for government cyber aggression, actors can do almost

---

[1] M Willett - Survival: October-November 2022 and undefined 2023, "The Cyber Dimension of the Russia–Ukraine War," *Taylorfrancis.Com*, accessed November 11, 2024, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003422211-1/cyber-dimension-russia–ukraine-war-marcus-willett.

[2] U Priyono Pertahanan, "Cyber Warfare as Part of Russia and Ukraine Conflict," *Pdfs.Semanticscholar.Org*, 2023, https://pdfs.semanticscholar.org/9c41/60f02d04ccff4b5eed16ea54051af059ee2a.pdf.

anything they want. This impunity for Russia has made it possible to carry out its geopolitical aims with very little immediate consequence. The attack for the US and its allies has shown that we need strong international rules and improved unified defenses against increasing cyber-warfare.

In this paper, the NotPetya cyber-attack is considered from the perspective of realist theory in IR: why, how and what does it mean for the states involved? It discusses the ways in which Russia utilized cyberspace as a tool of asymmetric war in pursuit of strategic advantage without direct military intervention. The report also discusses Ukraine's struggles for independence and strength against cyber threats and how foreign assistance is necessary to protect its borders. And finally, the paper examines how the United States responds to Russian aggression in the service of national security and maintains global cyber security supremacy3.

Examining the governments' official policies and tactical reactions, this article demonstrates the centrality of power, security and state action in the anarchic and ever more fractious space of cyberspace. The NotPetya attack is a great example of how cyber operations are changing the game of global warfare,4 and shows how this new realm of conflict opens up both possibilities and threats. In doing so, the article contributes to a better appreciation of the implications of cyber war for world order and the changes in the state relations in the modern digital era.

Research Questions

How did the NotPetya cyber-attack – which emerged from the Russia-Ukraine war – affect the cyber security posture and policies of the US?

Which US economic and technological loopholes were uncovered or tapped by the NotPetya cyber-attack?

How significant was the NotPetya attack as an initiator of international cyber security cooperation or rivalry, notably between the US, Ukraine and Russia?

Theoretical Framework

Realism: Cyber security in an Anarchic World. Realists offer an enabling frame for viewing the NotPetya cyber-attack as a means of statecraft in an anarchic international order. Realists treat the world as a war for power and security. We see the NotPetya attack as a strategy by Russia to conquer Ukraine and to confront the wider Western

---

[3] Theodoros Komninos and Dimitrios Serpanos, "Cyberwarfare in Ukraine," *Hybrid Threats, Cyberterrorism and Cyberwarfare*, September 30, 2023, 127–47, https://doi.org/10.1201/9781003314721-7/CYBERWARFARE-UKRAINE-THEODOROS-KOMNINOS-DIMITRIOS-SERPANOS.

[4] MS Dhelie et al., "Methods Used in Cyberattacks in the War Between Russia & Ukraine," 2023, https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3075261.

coalition, including the US. Russia was using cyber to undermine Ukraine's infrastructure and economy, as well as to show it could crash the international system. The NotPetya attack represents the cyber domain's security dilemma where defenses from one state become attacks from another. And the way the US and its allies responded to the attack, by increasing cyber security and placing sanctions on Russia only made matters worse and fed the cycles of distrust and escalated attacks.

Realist approach places the focus on states as central actors of international affairs. For this reason, the NotPetya attack underscores Russia's asymmetrical warfare in the service of geopolitical goals. It also underlines the U.S.'s high concern for national security in cyberspace by attempting to discourage future cyber-attacks with policy and technology.5 States of the anarchic international order use self-help to survive. The NotPetya case drove the US to rake in money for cyber security as a realist response to a looming existential crisis. This emphasis on self-reliance fits with the realist maxim of prioritizing national security over international cooperation in matters where a lot depends on it.

The NotPetya Cyber-Attack through the Realist Lens

According to realists, the international order is anarchic – states are major actors acting in the national interests. The NotPetya cyber-attack was orchestrated by Russia to gain an edge in geopolitical conflict with Ukraine and the West. Russia used Ukrainian infrastructure to weaken its ally economically and politically, threatening its sovereignty and its statehood6.

Cyber-attacks such as NotPetya enable states to project power asymmetrically. Economic sanctions and traditional military impediments left Russia using its cyber assets to gain influence in the region and overthrow U.S.-dominated global power 7

Realists draw attention to the security problem, in which states' countervailing actions instil insecurity in others. On a realist level, Russia understood Ukraine's participation in Western alliance's such as NATO and the European Union as a direct challenge to its area of influence. The cyber-attack had been preemptive of this invasion.

As a result of viewing the attack as a more widespread threat to international security, the U.S. and its allies reacted by doubling down on cyber security investments and

---

[5] T Komninos et al., "Cyberwarfare in Ukraine: Incidents, Tools and Methods," *Taylorfrancis.Com*, accessed November 11, 2024, https://www.taylorfrancis.com/chapters/edit/10.1201/9781003314721-7/cyberwarfare-ukraine-theodoros-komninos-dimitrios-serpanos.

[6] Dominika Kunertova, "The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game," *Bulletin of the Atomic Scientists* 79, no. 2 (2023): 95–102, https://doi.org/10.1080/00963402.2023.2178180.

[7] (Brantly et al., 2023)

sanctioning Russia. All of these measures fed Russian anxieties of circling, driving further distrust and expansion8.

In a true anarchy, states focus on survival and depend on self-help: This is the reality of reality. Russia could not effectively fight back militarily against the U.S. and its allies, so asymmetric means such as cyber-attacks served the purpose. NotPetya showed how Russia could harness the weaknesses of commingled world systems to cause mass destruction.

The United States beefed up cyber security protections as cyber wars escalated. This is explained by reality as a justified step to secure national security and deter further assaults. Realism tells us that states are determined to preserve or change the power dynamic so that they can be safe 9

The NotPetya attack highlights Russia's attempt to preserve its position in Eastern Europe through a crisis in Ukraine and a confrontation with the West. The attack also revealed how power was shifting in the international order as cyber is increasingly as important as conventional military equipment. The American and allied responses sought to rebalance the scales through their power of resilience and revenge.

The US used diplomatic, economic and cyber-reactions to prevent future violence. Sanctions against Russian entities warned against future cyber-attacks against U.S. interests. The attack was also a piece of coercive diplomacy on the part of Russia, who was ready to deploy cyber forces in the service of geopolitical objectives like manipulating Ukraine's domestic affairs and scaring off its West-centric orientation 10.

The cyber space is not well-governed globally and thus a target of states' competition. Russia took advantage of this absence of rule to stage the NotPetya attack in good faith. Realistically, the attribution problem is difficult in cyberspace, where states can carry out opportunistic activities and remain unaccountable to themselves – making deterrence harder still.

In the realist sense, the NotPetya attack only escalated the US-Russia adversarial relationship. The strike is part of a larger race between the United States and Russia in their competition to dominate the multipolar world order 11

---

[8] Mark Grzegorzewski, "Russia's 2022 Cyber-Enabled Warfare Against Ukraine: Why Russia Failed to Perform to Expectations," *The Great Power Competition Volume 5*, 2023, 47–73, https://doi.org/10.1007/978-3-031-40451-1_4.

[9] Dhelie et al., "Methods Used in Cyberattacks in the War Between Russia & Ukraine."

[10] Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," *Survival* 64, no. 5 (2022): 7–26, https://doi.org/10.1080/00396338.2022.2126193.

[11] Pertahanan, "Cyber Warfare as Part of Russia and Ukraine Conflict."

U.S. actions (public blame and sanctions) aimed to cement the US position as world power and rebuff Russian aggression. The NotPetya attack demonstrates how cyber warfare becomes part of hybrid warfare, where conventional military means are mixed with unconventional methods to serve state goals. The attack triggered a cyber-arms race, in which states are spending a lot of money to protect themselves with both offensive and defensive cyber tools.

Official Policies of Russia, Ukraine and USA

1. US Policy:

The United States presented the NotPetya attack as a part of Russia's larger geopolitical planning, and responded by means of both defense and attack.

The Russian military (GRU) was responsible for the attack — which the U.S. declared a state-backed cyber-attack. This public attribution was a step in the direction of openness in the battle against cyber adversaries. Russia – not just NotPetya-related individuals and organizations – are also sanctioned by the US in 2018. Such steps were meant to discourage more cyber-crime12.

US has updated cybersecurity policy to keep up with changing cyber threats. As the National Cybersecurity Strategy 2023 highlights, boosting critical infrastructure resilience, establishing public-private partnerships to limit risks, Partnering with other nations to define cyber standards and enhance cyber defenses worldwide.

The U.S. technical and financial assistance was extended to Ukraine to enhance its cyber security. Initiatives include: Cooperation exercises and training courses for cyber security strengthening of Ukraine, Cyber Threat detection and Response — Information sharing with Ukraine to protect themselves from cyber-attacks13. The US has become more actively engaged in offensive cyber strategies as part of its defense strategy, and is ready to attack cyber enemies if national security is at stake.

2. Ukrainian Policy:

Ukraine was the main victim of the NotPetya attack, so its reaction aimed at reducing the casualties and avoiding the next one. Ukraine declared the NotPetya strike in Russian hybrid warfare against Ukraine. Operations began with disaster response to restart vital functions and stop the spread of the malware. Ukraine created a national cyber security strategy consisting of:

Building cyber defence teams in its military and intelligence service.

---

[12] V Weber, "Why Great Powers Launch Destructive Cyber Operations and What to Do About It," 2023, https://www.ssoar.info/ssoar/handle/document/91327.

[13] A Salt, M Sobchuk - Canadian Global Affairs Insfitute, and Undefined 2021, "Russian Cyber-Operations in Ukraine and the Implications for NATO," *Cgai.Ca*, 2023, https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato.

Re-inventing its essential systems to prevent cyber-attacks.
Work with private sector experts to protect government systems.
International Collaboration.
Ukraine cooperated with NATO, the European Union, and NATO allies such as the US and Denmark in building cyber-machines. For example: NATO supported the cyber incident response via its Cooperative Cyber Defense Centre of Excellence (CCDCOE). Collaboration and training of Ukrainian cyber experts were also possible under bilateral arrangements. Even now Ukraine is still prone to hackers. Another massive attack was launched against Ukraine's state registry in December 2024, and this is where Russian cyber war has been going on for too long 14
3. Russian Policy
Russian cyberspace policies and conduct express its political and statecraft approach to cyber assets. Russia claims to be behind the NotPetya attack, but its cyber activities fit with its geopolitical aims15.
Cyber Operations Doctrine:
For Russia, cyberspace is a space where power is projected and strategic objectives are pursued without direct war. Russian military doctrine focuses on cyber-enabled hybrid wars that can hack into opponents' systems and turn people against you. Russia has never owned the NotPetya attack and other cyber-attacks. This plausible deniability complicates international reactions and frees Russia from direct responsibility.
Impact of Sanctions:
Sanctions from the international community, such as from the US and European Union, have targeted Russian cyber operations. Such sanctions have limited some Russian activities, but not cyber-crime more broadly. Russia is still spending a lot of money on its cyber arsenal in the form of attack equipment and disinformation operations. These are part of its wider annexation strategy of rebuffing Western influence and retaining its regional authority 16

Key Policy Implications and Trends worldwide

Shift toward Cyber Norms the NotPetya attack has pushed the world into a new debate about how states ought to act in cyberspace. Work by the UN and other international organizations tries to provide systems for accountability and conflict resolution.
Cyber Arms Race the hack shows how cyber abilities have become central to US national security strategies. Both the U.S. and Russia increased investments in offensive and defensive cyber tools to promote a cyber-arms race.

[14] (Komninos et al., 2023)
[15] Pertahanan, "Cyber Warfare as Part of Russia and Ukraine Conflict."
[16] (Firdini et al., 2024)

Hybrid Warfare Context NotPetya is an example of hybrid warfare where cyber activity runs in parallel to traditional wars. This blend reveals how war and peace have lost their separate boundaries in the 21st century.

Global Economic Impacts the extent of the attack – which hit large companies and supply chains around the world – showed how intertwined cyber threats are. The result is that both governments and companies have had to rededicate themselves to cyber security17.

Discussion

The NotPetya cyber-attack – a case study of state-backed cyber aggression – highlights how power and conflict change over time. This is done from IR's realist perspective: we look at the reasons, options and impacts for the protagonists: Russia, Ukraine and the US. Realist politics, with its focus on strength, security and the anarchic character of the global order, is an attractive vehicle for considering this episode and its geopolitical consequences. This example is not just about the realities of cyber warfare, it is also about how technological creativity and conventional statecraft work together to create world security.

Russia's Cyber Warfare Strategy.

Russia's role in the NotPetya attack fits into its larger hybrid warfare strategy, where conventional and non-conventional tools are used to achieve a purpose. Realistically, Russia does what it does because it wants to keep regional control, to undermine Western authority and claim the global stage. Among its purposes in taking on Ukraine was to economically and politically destabilize its neighbor, undermining Kyiv's attempts to join Western forces like NATO and the European Union. The terrorist attack knocked out electricity and banking infrastructure, devastating economic output and weakening public trust in Ukraine's leadership.

The attack was also a manifestation of Russia's cyber-power, and it showed that it can disrupt rivals globally. Such a projection of power is in line with realist thinking about how capabilities serve to dissuade competitors and affect global relations. Then there was the fact that the cyber warfare is vague and the reasons for it are highly questionable, so Russia was able to carry out its goals with plausible deniability, while not incurring any direct cost and getting as much strategic advantage as possible. The strategic messages included in the attacks also established Russia as a potent cyber threat with the potential to shift world security thinking.

Ukraine's Resilience and Strategic Responses

[17] Weber, "Why Great Powers Launch Destructive Cyber Operations and What to Do About It."

Ukraine's reaction to the NotPetya assault shows the difficulty of weaker states in asymmetric warfare. Realist theory says that such states will seek alliances and aid from the outside to counter stronger enemies. Ukraine's dependency on Western help, from cyber security training to technology and intelligence, has been essential here to strengthening its defences against more aggression. Cooperation with organizations like NATO's Cooperative Cyber Defence Centre of Excellence and with private cyber security companies have facilitated the correction of immediate holes.

Ukraine, with very few resources, has already improved cyber security capabilities and stepped up international collaboration.18 These efforts are based on a realist conception of how to respond to emerging security risks and draw upon resources to protect sovereignty. But the attack revealed systemic weakness too, and shows the need for long-term investment and institutional reform. The Ukrainian flexibility and attempt to conform to the global cyber standards is a tactical change in Ukraine's security policy.

The US: How to Find a Balance between Deterrence and Defense.

US was not the direct victim of NotPetya, but they were collateral losses for large corporations and infrastructure. In realist terms, this event reinforcing the US's view of Russia as a strategic rival, and an evidence of the interconnected nature of contemporary security issues. The economic cost of the attack – billions in losses in shipping, logistics and healthcare sectors – demonstrated just how weak an interconnected global economy could be.

Washington has followed up with a two-pronged approach, deterring adversaries and beefing up its cyber protections. The US official policies – sanctions against Russian companies and actors in the cyber war – have realist rationales of power symmetry and defiance. These sanctions are meant to punish Russia, preventing similar strikes in the future, and also to assure US allies that the US is still here for them. At the same time, the US has spent billions of dollars on improving its cyber security, public-private partnerships, and encouraging international best practices to combat the increasing risks of cyber warfare.

In addition, the US Department of Defense Cyber Strategy emphasizes the need to be proactive – to protect before they're too late. The doctrine also indicates an increasingly offensive cyber strategy for deterrence, and a need to preserve technological lead in an era of ever increasing cyber warfare.

---

[18] M Grzegorzewski - The Great Power Competition Volume 5: The Russian and undefined 2023, "Russia's 2022 Cyber-Enabled Warfare Against Ukraine: Why Russia Failed to Perform to Expectations," *Springer*, accessed November 11, 2024, https://link.springer.com/chapter/10.1007/978-3-031-40451-1_4.

What This Means for International Law and Governance

NotPetya is also another reminder of the limitations of current international arrangements for cyber warfare. The absence of uniform rules and regulations opens up cyberspace to the sort of strategic possibilities that are available to both states and non-state actors. Realism – which emphasizes the chaos of the international order – anticipates this behavior when there is no centralized authority. With no agreed-upon cyber rules of conduct, escalation and risk-taking in this volatile field are only exacerbated.19

The attempt to develop international cyber norms – efforts led by the UN and regional organizations for example – have been muted because states have differing interests and power imbalances. Russians' fight for cyber-state sovereignty, for example, and Western demand for open and interoperable networks — in other words — are reflections of geopolitical rivalries.20 The realist argument points to the challenge of negotiating consensus in a fiercely competitive international community where states care about national interests' more than common security. There is no good mechanism for attribution, making accountability further hard to enforce and allowing the perpetrators to get away with it, and so on.

The Impact of the NotPetya Cyber-Attack on Regional Economies

The worst impact came from Ukraine in the form of the NotPetya attack, which messed up the economy on several fronts. Malware damaged important infrastructure, such as power grids, traffic systems, and government operations. The loss of critical services dented business activity, at a cost of hundreds of millions of dollars.21

Banking operations in Ukrainian banks remained crippled due to the attack. This undermined public trust in the financial system, which reduced spending and economic growth. Many Ukrainian companies went through a long period of downtime with revenue loss, supply chain disruptions and additional expenses for recovery and cyber security protection.22

The strike made Ukraine's already precarious economic situation worse, and made the ongoing war with Russia cost even more.

Spillover Effects on Neighboring Economies

---

[19] M Baezner, "Cyber and Information Warfare in the Ukrainian Conflict," 2018, https://www.research-collection.ethz.ch/handle/20.500.11850/321570.

[20] Brantly, Security, and 2024, "The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations during Russia's War on Ukraine."

[21] Komninos et al., "Cyberwarfare in Ukraine: Incidents, Tools and Methods."

[22] Willett, "The Cyber Dimension of the Russia–Ukraine War."

Although Ukraine was the main target, the attack's outreach showed how weak are economies located close to Ukraine's economic infrastructure.

Eastern Europe: Poland and the Baltic countries, which have a deep trade and investment relationship with Ukraine, had to pay an indirect economic price. Supply-chain interruptions – particularly manufacturing and logistics – limited cross-border transactions.
Impact in Energy Industry: The strike's destruction of energy providers, such as Ukraine's power grid, also rippled out to energy exports to the rest of the world – short-term depletions and shocks to the price.
Banks: In-neighboring banks were exposed to more cyber-attacks after NotPetya had notified them about system failures. Expenditure on cyber security stretched emerging economies' resources.
Global Business Losses with Local Implications.
NotPetya was no longer restricted to Ukraine and its immediate neighbors, but also affected multinational corporations based in the area. Maersk, Merck and FedEx's European unit, TNT Express, all remunerated billions in losses; the global damage was estimated at more than $10 billion. These losses were regionally consequential:
Merchandise and Transport: Maersk's suspension of shipping clogged up European ports, affecting European trade and spiking the prices of firms who depend on timely deliveries.23
Pharma Industry: The production and distribution delays experienced by Merck hit health care infrastructure in Eastern Europe, showing the fragility of digitally based supply chains.
Insurance and Risk Management: The attack caused cyber risk to be reconsidered by insurance companies and subsequently, policies were more expensive and cover terms more restrictive, particularly for small businesses in the area.24
Strategic Vulnerabilities Exposed, NotPetya revealed the weaknesses in digital infrastructure of regional economies and points out. Most organizations and government were not prepared for this attack because they had weak cyber security systems that are not ready for the scale and complexity of the attack.

[23] M Thakur - Journal of Applied Science and Education (JASE) and undefined 2024, "Cyber Security Threats and Countermeasures in Digital Age," *Jase.A2zjournals.Com* 04, no. 042 (2024): 1–20, https://doi.org/10.54060/a2zjourna.
[24] 2022 and 2023, "The Cyber Dimension of the Russia–Ukraine War."

Network-Connected Systems: The dependence on shared networks and third-party applications (such as the hacked M.E.Doc accounting software) enhanced the effect of the attack because a single point of failure spread through systems with each other.25
Economic Dependencies: Regional dependence on Ukrainian infrastructure and economy left neighboring countries vulnerable to indirect risks, hence requiring shared cyber security policies.

Long-Term Economic Implications
More Cyber security Investments: Governments and corporations in Eastern Europe and beyond have since invested large amounts of money in cyber security. These measures are necessary but take money away from other developmental projects and could derail growth.
Lower Investors' Belief: The attack caused alarm over the future of the digital and economic landscape of the region, which discouraged foreign investment and made it difficult to draw in multinational companies.26
Changes in policy: As the attack forced local governments to rethink how they handle cyber risk, new regulations and programs for better resilience came into play. But those measures typically fall short of the dynamism of cyber-attacks.
The economic harm caused to Ukraine and the rest of its neighbors reflects on how state sovereignty becomes undermining in cyber-space where conventional boundaries have only weak immunity.

Conclusion

What we can learn from the NotPetya event, strategically, for states dealing with cyber conflict. States need to make investment in advanced cyber security to safeguard critical infrastructure and mitigate vulnerabilities. That means cooperation between governments, private actors and international stakeholders.
A strong deterrence model that is a blend of defensive, offensive and signaling capabilities is needed to stop adversaries from engaging in cyber-attacks. Although tough, the work to establish consensus about cyber norms and create attribution and accountability are still essential to the management of cyber conflict.27
Cyber threats require constant innovation and adaptation, and must also be integrated into the overall national security environment. Ensuring that government and private

[25] Firdini, …, and 2024, "The Role of Russian Cyber Operations in The Russian–Ukraine War in Achieving Russia's Strategic Objectives."
[26] Grzegorzewski, "Russia's 2022 Cyber-Enabled Warfare Against Ukraine: Why Russia Failed to Perform to Expectations."
[27] Salt, Insfitute, and 2021, "Russian Cyber-Operations in Ukraine and the Implications for NATO."

organizations are better co-operating on threat intelligence and rapid response is essential. Developing an educated workforce that is prepared to respond to new cyber threats is critical for sustaining long-term resilience and competitive advantage.28

The NotPetya cyber-attack illustrates once again the transformative power of cyber operations on the world stage. By virtue of realist theory, this episode shows just how crucial power, security and state action are to shaping global relations. In the eyes of Russia, Ukraine and the United States, the attack made the strategic importance of cyberspace as a zone of competition and conflict clear. The outpouring of the attack also revealed how globally interconnected global infrastructures are, and how dangerous cyber threats are.29

In an age of a global order being confronted with cyber war, NotPetya will continue to be influential for how future policies and solutions will keep the world in check in an ever more volatile arena. Deterrence and the establishment of strong global rules and the improvement of social resilience are key to preventing cyber wars and preserving the integrity of the digital ecosystem.30

The NotPetya cyber-attack provides an example of how the cyber toolbox has been applied effectively in modern international relations. The American, Ukrainian and Russian responses are an expression of their respective cyber-plans. In the case of the United States and Ukraine, it has been about building forces, forming coalitions and scaring away attacks. Cyber is, and always will be, an integral component of Russia's geopolitical toolkit to attack adversaries and impose their will in a digitalized world.31

---

[28] Komninos et al., "Cyberwarfare in Ukraine: Incidents, Tools and Methods."

[29] Weber, "Why Great Powers Launch Destructive Cyber Operations and What to Do About It."

[30] Aaron F. Brantly and Nataliya D. Brantly, "The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations during Russia's War on Ukraine," *Intelligence and National Security* 39, no. 3 (2024): 475–95, https://doi.org/10.1080/02684527.2024.2321693.

[31] (JASE) and 2024, "Cyber Security Threats and Countermeasures in Digital Age."