Ukraine Russia Crisis: Terrorism Briefing

- Ukraine, Russia Crisis
- Conflict & Terrorism
- Impact of Cyberattacks
- The Spillover Threat

Institute for Economics & Peace

Quantifying Peace and its Benefits

The Institute for Economics & Peace (IEP) is an independent, non-partisan, non-profit think tank dedicated to shifting the world's focus to peace as a positive, achievable, and tangible measure of human well-being and progress.

IEP achieves its goals by developing new conceptual frameworks to define peacefulness; providing metrics for measuring peace; and uncovering the relationships between business, peace and prosperity as well as promoting a better understanding of the cultural, economic and political factors that create peace.

IEP is headquartered in Sydney, with offices in New York, The Hague, Mexico City, Brussels and Harare. It works with a wide range of partners internationally and collaborates with intergovernmental organisations on measuring and communicating the economic value of peace.

For more information visit www.economicsandpeace.org

Please cite this report as:
Institute for Economics & Peace. The Ukraine Russia Crisis: Terrorism Briefing, Sydney, March 2022.
Available from: http://visionofhumanity.org/resources (accessed Date Month Year).

UKRAINE RUSSIA CRISIS: TERRORISM BRIEFING

On 24 February 2022, Russia launched an attack on Ukraine. Figure 1 highlights that the invasion comes after a decade of deteriorating relations between Russia, Ukraine and the West.

This brief covers several aspects relating to the current Ukrainian war, including the frequency of past acts of terrorism in Russia, Ukraine and Georgia and covers likely future scenarios. It also analyses cyberattacks on Ukraine over the last decade and lead up to the current war.

The main finding is that terrorism increases with the intensity of conflict. Both the Georgian conflict in 2008 and the Ukrainian conflict of 2014 saw substantial spikes in terrorist activity around the wars, and as the current war intensifies increased terrorist activity should be expected.

Secondly, cyberattacks on Ukraine have markedly increased over the last decade, and especially in the months and weeks leading up to the war. Further, cyberattacks have the potential to unintentionally spill over into other countries because of global connectivity, the effects of which have been seen on numerous occasions. As cyberattacks by nefarious actors are a recent phenomenon, and given the difficulty in the attribution of such attacks, the demarcation between what constitutes a cyberattack, cyber warfare or cyber terrorism are unclear. Regardless, this briefing looks at the broad phenomena of cyberattacks in Ukraine to offer background on recent events.

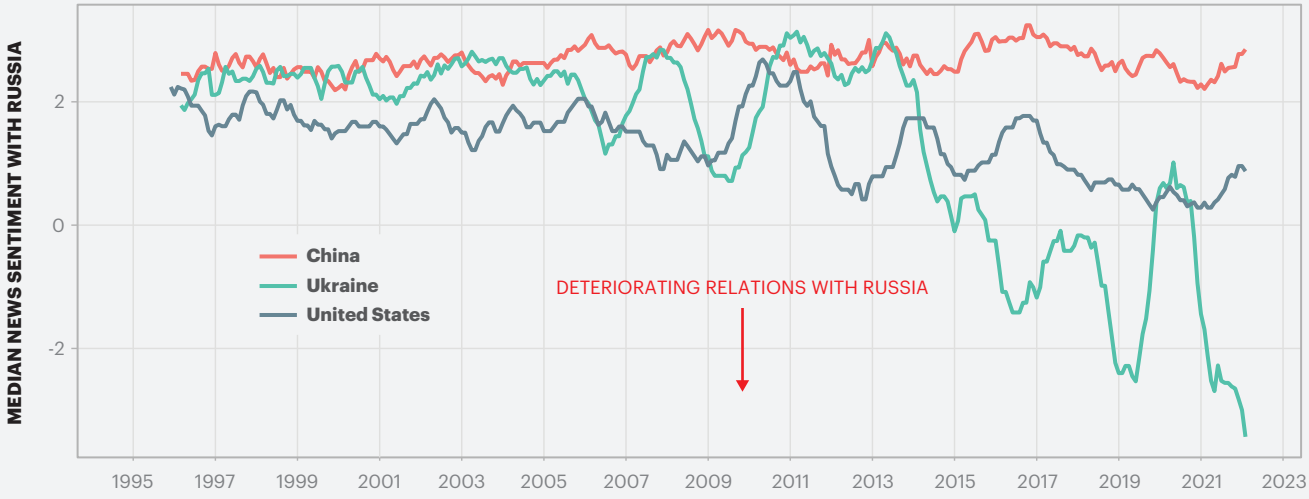
HIGHLIGHTS

- There is a strong relation between terrorism and conflict, with 97 per cent of all terrorist deaths recorded in a conflict zone.
- Terrorism deaths in Ukraine are expected to increase substantially in the coming months and will rise proportionally with the intensity of the conflict.
- This is despite terrorism in Russia and Ukraine improving - in Russia since 2012 and the Ukraine since 2015.
- Terrorist attacks in Russia had been declining since 2012 when 213 attacks were recorded. In 2021 there was only one.
- Terrorist attacks in Ukraine peaked in 2015 with 58 attacks, while in 2021 there were none.
- Terrorist deaths in Ukraine peaked during 2014 conflict with Russia.
- Terrorism peaked in the Russia and Eurasia region in 2010 in the wake of the Russian-Georgia conflict with 339 attacks and 318 deaths recorded.
- The period between the conflict with Georgia and the annexation of Crimea accounted for the most terrorism in Russia over the last two decades with 87 per cent of attacks and fatalities occurring between 2008 and 2014.
- Russia, Ukraine and Belarus were the only countries in the region to record over one thousand violent demonstrations in 2021.

FIGURE 1

Russian relations

Russian relations with Ukraine and the United States have deteriorated in the past decade while relations with China have remained stable.



Source: ICEWS

TERRORISM IN RUSSIA, UKRAINE AND GEORGIA

Terrorism in Ukraine and Georgia has been predominately associated with the 2008 and 2014 conflicts with Russia. Outside of these two periods, terrorism in both countries has been low. If past patterns are any indication, then terrorist activity would be expected to increase markedly with the current conflict. Generally, the level of terrorism is proportional to the intensity of the conflict. Terrorist attacks are also a commonly used tactic in asymmetric warfare, usually targeting military, police and government infrastructure. If Russia gains control and appoints a puppet government, it will most likely meet with strong resistance and face a sustained insurgency. Myanmar is a case in point where after the democratically elected government was overthrown in 2021 by a military coup. Following this terrorism increased 23 times, resulting in 521 deaths, up from 23 deaths.

Over the last six years, terrorism in the Russia and Eurasia region has declined. Ninety-three per cent of the region's attacks since 2007 were recorded prior to 2016, highlighting how pronounced this decline has been. Terrorism peaked in the region in 2010 in the wake of the Russian-Georgia conflict, with 339 attacks and 318 deaths recorded in that year.

Since 2007, the most active terrorist group in the region was Shariat Jamaat and its affiliates which recorded 315 attacks and 257 deaths, mostly occurring in Russia. They were followed by the Caucasus Emirate with 39 attacks and 134 deaths attributed to the group.

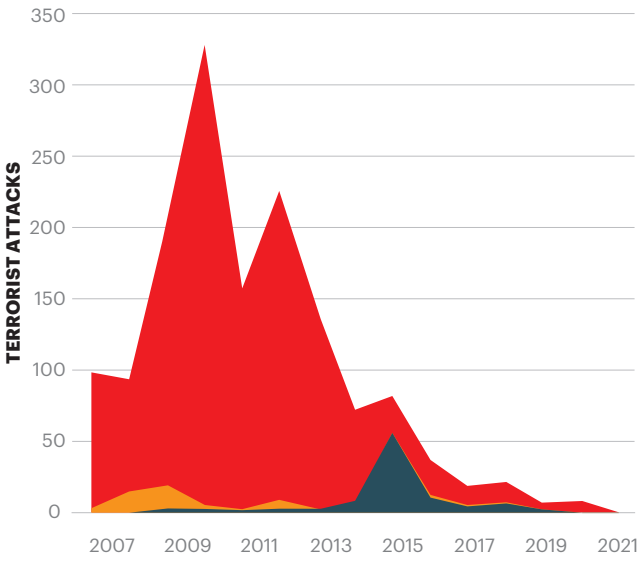
While it is a jihadist group primarily, Shariat Jamaat is also known as Vilayat Dagestan, is also closely associated with the separatist conflicts in the Russian republics of Chechnya and Ingushetia. Shariat Jamaat also maintained links to the Caucasus Emirate. The group ceased to be operational after the deaths of successive leaders from Russian special forces. Islamic State (IS) has also been active in the region over the last two decades with 36 attacks and 102 deaths recorded since 2007.

Most attacks were not claimed by any recognised terrorist group with 1,122 attacks and 846 deaths attributed to unknown groups or 73 per cent of attacks.

FIGURE 2

Terrorist attacks in Russia, Georgia and Ukraine, 2007–2021

Ninety-three per cent of attacks in the region occured before 2016.

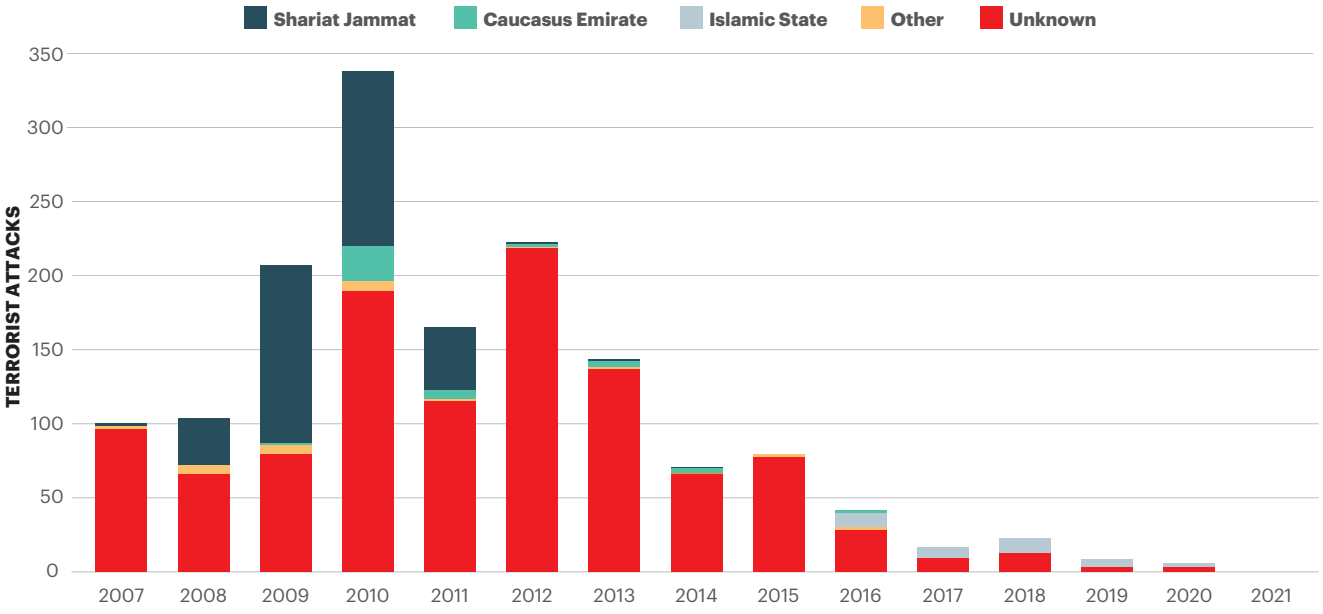


Source: Dragonfly TerrorismTracker, IEP calculations

FIGURE 3

Number of attacks by group in Russia and Eurasia region, 2007–2021

Shariat Jammat was the most active group in the region.



Source: Dragonfly TerrorismTracker, IEP calculations

Russia has almost consistently had the highest number of terrorist attacks and deaths in the region, with 1,312 attacks and 1,179 deaths recorded since 2007. Attacks and deaths in Russia have declined consistently over the last decade with only one attack and two deaths in 2021.

The period between the conflict with Georgia and annexation of Crimea accounted for the most terrorism in Russia over the last two decades with 87 per cent of attacks and fatalities occurring between 2008 and 2014. Terrorism in Georgia mirrors the Russian trend, with 90 per cent of terror attacks recorded occurring during the same period.

Ukraine accounts for the second highest number of attacks in the region since 2007, recording 108 attacks, resulting in 17 deaths. Attacks and deaths peaked in 2015 at 58 attacks and ten deaths, corresponding with conflict with Russia.

Since the peak, there has been a fairly consistent decline with no attacks recorded in Ukraine in 2021 and only one in 2020. Since 2007 only one attack has been claimed by a group – Odessa Underground; the remaining 107 attacks were not claimed by any known group.

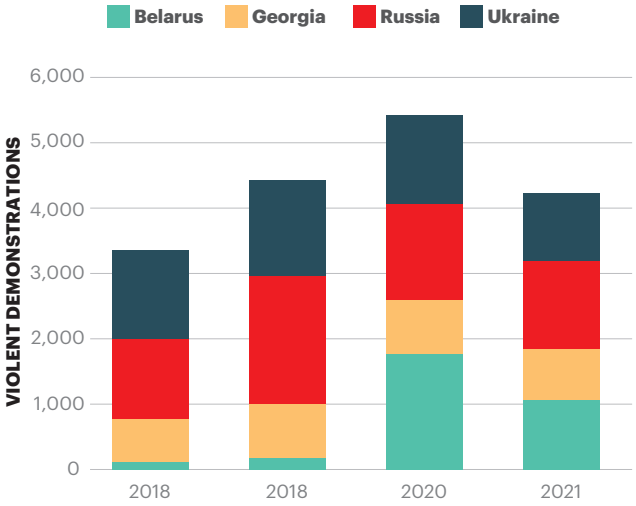
The trend in violent demonstrations reflects the global trend where demonstrations rose by 10 per cent per annum in the decade to 2020.

Despite dropping by nine per cent in 2021, Russia continues to have the highest number of violent protests and riots in the region, at 1,337 incidents. Ukraine followed with 1,052 incidents in 2021, a decrease of 23 per cent from the year before.

FIGURE 4

Violent demonstrations by country, 2018–2021

Russia recorded the most violent demonstrations followed Ukraine.



Source: ACLED, IEP calculations

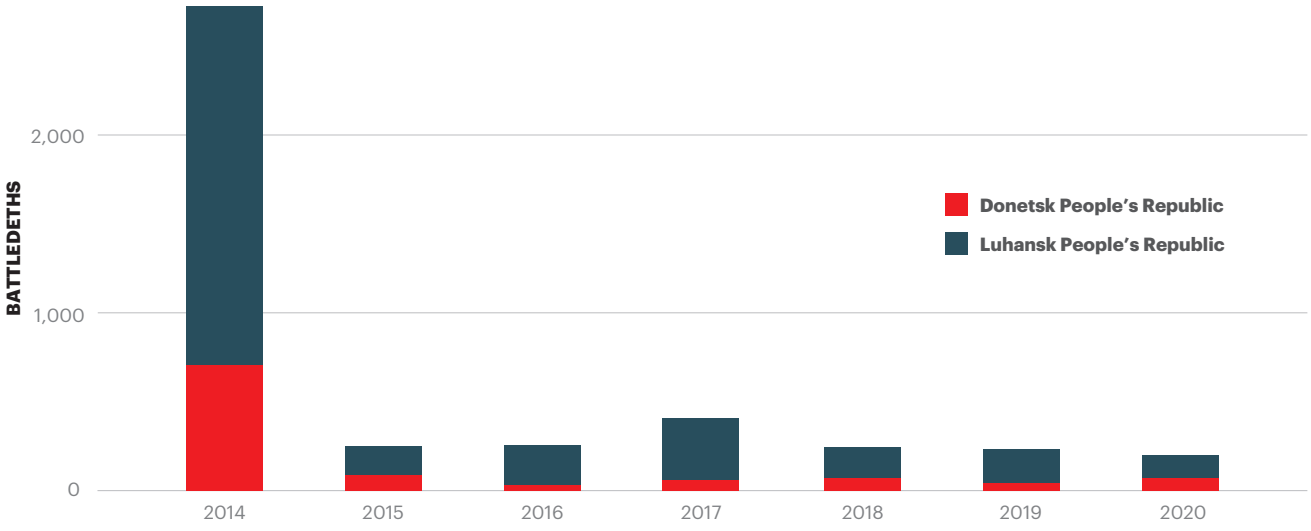
Russia, Ukraine and Belarus were the only countries in the Russia and Eurasia region to record over one thousand violent demonstrations in 2021.

Separatist insurgency groups have also been active in Eastern Ukraine. Since 2014, conflicts involving The Donetsk People's Republic (DPR) and Luhansk People's Republic (LHR) recorded over 4,000 battle deaths. Activity peaked in 2014 recording slightly under 3,000 battle deaths in that year.

FIGURE 5

Separatist groups in Donbas, 2014–2020

Conflicts involving the Donetsk People's Republic and Luhansk People's Republic have recorded over 4,000 battle deaths since 2014, though activity has been lower over the past few years.



Source: UCDP, IEP calculations

BOX 1

Ukraine, Donbas conflict and the extreme far-right

Some estimates suggest that the conflict in Donbas has claimed the lives of over 13,000 Ukrainians and the displacement of a further 1.5 million.[1] It has also served as a magnet for many far-right extremists looking to gain experience in weapon training and fighting, where they find groups such as the Azov Battalion, whose insignia (a 'sonnenrad' or sunwheel) appeared on the back of the Christchurch shooter's rucksack. The Battalion, prior to the Russian invasion, had around 10,000 members.

On 21 February 2022, Russian propaganda recognised the independence of Donetsk and Luhansk and subsequently sent in 'peacekeeping forces' to help de-Nazify the Ukraine and 'save' ethnic Russians.

CYBERTERRORISM, UKRAINE CONFLICT AND RUSSIAN CYBERATTACKS

HIGHLIGHTS

- Cyberattacks in Ukraine have substantially increased over the last decade.
- Ukraine has been the target of many cyberattacks over the past years. In 2020, the number of attacks was close to 400,000.[2] Past high profile attacks in the Ukraine include NotPetya, CrushOverride, Cyclop Blink.
- The current war in Ukraine is likely to see cyberattacks become more prevalent.
- Ukrainian government has trained volunteer hackers to target Russia and Anonymous has also stated its intention to target Russia.
- The impact of cyberattacks can be much broader than their targets, spilling over into other countries. For example, while NotPetya targeted Ukraine, its effect was felt in the USA, UK, and Australia.

DEFINING CYBER WARFARE AND CYBER TERRORISM

The increased dependence on communications and information technology has meant that the online sphere has become of great interest to nefarious actors, giving rise to categorisations such as 'cyberattacks', 'cyber warfare' and 'cyberterrorism'. However, categorising any cyber incident into one of these three terms is problematic. Attribution is often difficult for any cyber incident as the sources of the attacks are often challenging to trace. Therefore, the perpetrator, motivation and intended purpose are often unclear. Without this, demarcation of what constitutes warfare (state actions) vs terrorism (non-state actions) is difficult. This confusion is at the heart of hybrid warfare where civilian and military tools, overt and covert operations are used to destabilise.

The cyber world is becoming one of the key battle spaces in which hybrid warfare are fought. NATO recognised cyberspace as the 5th battlespace at the Warsaw Summit in 2016 and a cyberattack as a potential Article 5 case which stipulates that an attack on one member is an attack on all. Currently Article 5 refers to a kinetic armed attack and is lacking a compatible cyber definition. Therefore, it will be up to the 30 NATO member states to define what amounts to a cyberwar after a cyberattack of sufficient strength.

Additionally, a conventional terrorist act is considered terrorism when the act is committed by a non-state actor with the aim of using violence or threatening violence, where the act sends a message to a broader audience than those affected by the violence. Therefore, attacks by the Russian government on the Ukrainian government, infrastructure or business would not be classified as an act of cyber terrorism. Outside of a conflict situation, classifying cyberattacks by governments as cyberattacks or cyber warfare is also not clear.

This paper does not attempt to answer these definitional questions, rather it looks at the previous attacks, the likelihood of future attacks and the unintended consequences from the flow-on effects to other countries.

Because of the increasing use of cyberattacks there is a need for the global community to improve the definitions of what constitutes cyber warfare, cyberterrorism or cyberattacks. The effects of this are profound as it will influence whether groups come under terrorist legislation, or whether an act of war has been declared. It is currently unclear, for example, under what circumstances a cyberattack on a NATO member would constitute an act of cyber warfare?

CYBERATTACKS IN UKRAINE

The unfolding crisis in Ukraine has called for greater focus on cyberattacks. Globally the number of cyberattacks has increased substantially over the last decade. It remains to be seen how extensively cyberattacks will be used in the current Ukrainian war. In the weeks before the conflict several sites had been attacked by Distributed Denial of Services (DDoS) attacks. Currently, the Ukrainian government is creating an international cyber army of volunteer hackers. Anonymous has declared cyber war on the Russian government. Within the first 24 hours, they claimed responsibility for disabling several Russian government websites.[3]

Ukraine has experienced persistent cyberattacks over the last decade, with many of the attacks attributed to Russia. In 2020, it faced 397,000 attacks and around 280,000 attacks in the first ten months of 2021.[4] The attacks were so extensive that the EU sent a Cyber Rapid Response Team to provide support.[5]

Russia, Cyberterrorism/Cyberattacks against Ukraine

Under President Putin, Russia has been credited with undertaking numerous cyberattacks globally. Such attacks can be initiated quickly, independently or in concurrence with other kinetic operations. They are also less dependent on time and distance and are relatively cheap to implement. Most importantly, they are exceptionally challenging to defend as they come in a variety of forms. Additionally, due to the interconnectivity of the web, malware can easily be inadvertently transferred to third parties for whom it wasn't intended.

Russia's use of cyberattacks began after the Russian withdrawal from Georgia in 2008.[6]

The increasing use of cyberattacks can be a leading indicator of something nefarious being planned. For instance, in January 2022, as diplomatic efforts were being ratcheted up, Ukraine experienced a widespread cyberattack on several government departments. The attack took the form of a message saying "Ukrainians! … All information about you has become public. Be afraid and expect the worse. It's your past, present and future." The message included a reproduction of the Ukraine flag and a crossed out map with a reference to "historical land".[7] Notably, soon after this attack, the Ministry of Defence came under DDoS attack, as did PrivatBank and Oschadbank, although the attack they faced was more about disinformation, claiming that their ATMs were not working.[8] The intention could have been to cause further panic.

Cyberattack operations are mainly carried out by the Russian Main Intelligence Directorate (GRU) and by entities that are officially unaffiliated to the Russian state, providing the government with an air of plausible deniability.

One early example of a Russian-led cyberattack occurred in December 2015 when Ukraine's industrial control systems networks were targeted by destructive malware causing power outages in the western Ivano-Frankivsk region; around 700,000 homes were without power for several hours.

A year later, Ukraine's power grid faced a malicious malware attack, called CrushOverride, which blacked out a portion of Kyiv's total power capacity for an hour.[9] The attack began when a 330-kilowatt sub-station was influenced by external sources who lay undetected within the IT system for six months, during which time they acquired more knowledge about the system.[10] This attack appears to have been a trial run by hackers wanting to test new malware that was directed against an electric power system. It is believed the malware could be fitted to target other critical infrastructure.

Russia continued to support cyberattacks, including the NotPetya attacks. The attacks deployed malware aimed at rendering data unusable. The malware was spread through tax software that companies and individuals require for filing taxes in Ukraine. The code was such that even if users did pay up, their data could never be recovered, which is why it was not ransomware as the purpose was destructive.

The malware spread to other countries, including the US. This led to the US Department of Justice charging six GRU officers with deploying the NotPetya ransomware, which affected hospitals and medical facilities around the world. The financial cost to the United States alone was around US$1 billion.[11]

Another example was Operation Exchange Marauder, where Russian hackers allegedly found a backdoor to Microsoft Exchange giving them access to email accounts and associated networks all over the world, including in Australia, the United States and Ukraine.

THE SPILLOVER THREAT

There is increased concern that cyberattacks will extend beyond Ukraine. Jeremy Fleming, Director of Government Communications Headquarters (GCHQ) has called on British critical infrastructure providers to be more vigilant.[12] The concern with a spillover situation is twofold. Firstly, when it comes to a cyberattack, there is no clarity as to how far it could reach because of the interconnectivity between individuals and entities. This was made abundantly clear with NotPetya or WannaCry.

Secondly, if the conflict is not unfolding as Russia had hoped, and it perceives the supply of weapons by European countries to Ukraine as hostile, it may order Russian hackers to extend their reach and look to cyberattacks to paralyse those opposing Russian efforts.

Several Baltic countries have faced cyberattacks from Russian sources. One example of a major attack, dubbed 'Ghostwriter', infected at least seven members of Germany's Bundestag parliament and 31 state parliamentarians were targeted. The attack began in Lithuania, Latvia, and Poland with the dissemination of disinformation aimed at promoting an anti-NATO agenda, before shifting to Germany.[13]

CONCLUDING REMARKS

Russia has clearly recognised the centrality of the cyber domain to attain global political goals, using affiliated and unaffiliated entities.

Cyberterrorism could be an effective tool for those wishing to achieve specific political goals that lack the resources to undertake targeted kinetic attacks against government buildings, institutions, or agencies.

Additionally, physical attacks by governments run the risk of starting a war, whereas there is less clarity when a cyberattack is significant enough to declare war.

Because of global interconnectedness cyberattacks have the potential of blending into mainstream society and causing widespread destruction and panic, particularly if the attacker has penetrated the system, with the malware lying in wait until an opportune moment to unleash the harm.

The danger with cyberterrorism and the growing pervasiveness of cyberattacks is that, just like violence, societies can become used to it and factor it in as a cost of living. This however raises unsettling prospects: by normalising cyberattacks by not taking adequate actions against the perpetrators, it makes further attacks more likely with all sides exhibiting greater willingness to unleash them on adversaries.

ENDNOTES

1 "Death Toll Up To 13,000 In Ukraine Conflict, Says UN Rights Office." Accessed February 28, 2022. https://www.rferl.org/a/death-toll-up-to-13-000-in-ukraine-conflict-says-un-rights-office/29791647.html.

2 "Ukraine Hit by 'Massive' Cyber-Attack on Government Websites | Ukraine | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

3 "Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia | Ukraine | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

4 "Ukraine Hit by 'Massive' Cyber-Attack on Government Websites | Ukraine | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

5 "EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks | Politico | Accessed February 28, 2022. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/.

6 "Ukraine Hit by 'Massive' Cyber-Attack on Government Websites | Ukraine | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

7 "Ukraine Hit by 'Massive' Cyber-Attack on Government Websites | Ukraine | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

8 "Ukrainian Ministry of Defense Websites Hit by Cyberattack - POLITICO." Accessed February 28, 2022. https://www.politico.com/news/2022/02/15/ukrainian-ministry-of-defense-websites-hit-by-cyberattack-00009046.

9 "Crash Override Malware Took Down Ukraine's Power Grid Last December | WIRED." Accessed February 28, 2022. https://www.wired.com/story/crash-override-malware/.

10 "Ukraine's Power Outage Was a Cyber Attack: Ukrenergo | Reuters." Accessed February 28, 2022. https://www.reuters.com/article/us-ukraine-cyberattack-energy-idUSKBN1521BA.

11 "How the NotPetya Attack Is Reshaping Cyber Insurance." Accessed February 28, 2022. https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

12 "UK Firms Warned of Russian Cyberwar 'Spillover' from Ukraine | Cyberwar | The Guardian." Accessed February 28, 2022. https://www.theguardian.com/technology/2022/feb/23/uk-firms-warned-russia-cyberwar-spillover-ukraine-critical-infrastructure.

13 "Russia-Backed Hackers Target German Legislators: Report | News | DW | 26.03.2021." Accessed February 28, 2022. https://www.dw.com/en/russia-backed-hackers-target-german-legislators-report/a-57018097.

Our research analyses peace and its economic value.

We develop global and national indices, calculate the economic impact of violence, analyse country level risk and have developed an empirical framework for Positive Peace that provides a roadmap to overcome adversity and conflict, helping to build and sustain lasting peace.

Download our latest reports and research briefs for free at:
visionofhumanity.org/resources

FOR MORE INFORMATION
INFO@ECONOMICSANDPEACE.ORG
EXPLORE OUR WORK
WWW.ECONOMICSANDPEACE.ORG AND
WWW.VISIONOFHUMANITY.ORG

GlobalPeaceIndex

@GlobPeaceIndex
@IndicedePaz

IEP is an independent, non-partisan, non-profit think tank dedicated to shifting the world's focus to peace as a positive, achievable, and tangible measure of human well-being and progress.

IEP is headquartered in Sydney, with offices in New York, The Hague, Mexico City, Harare and Brussels. It works with a wide range of partners internationally and collaborates with intergovernmental organisations on measuring and communicating the economic value of peace.