Gray zone aggression is an attractive option for Western rivals because it exploits the openness of Western societies. (American Society for International Law; Hybrid Warfare: Aggression and Coercion in the Gray Zone, November 29, 2017)

Countering Aggression in the Gray Zone

By Elisabeth Braw

In recent years, much has been written and said about conflict in the so-called "gray zone," often described as conflict below the threshold of combat. Gray zone aggression is an attractive option for Western rivals because it exploits the openness of Western societies. The fact that Western countries are characterized by small governments with limited powers to dictate the activities of their populations and businesses makes these countries even more attractive targets for nonkinetic aggression, ranging from hostile business activities, to cyber attacks, to kidnappings, assassinations, and even occupation by unofficial militias aligned with foreign powers. Resourceful adversaries use such actions to force wedges into the fault lines of open societies. With innovative thinking, however, liberal democracies can develop effective gray zone deterrence while staying within the norms of behavior they have set for themselves.

The Case of Sergey Skripal

On March 4, 2018, former Russian intelligence officer Sergey Skripal and his daughter Yulia were found in "an extremely serious condition" on a park bench in the English cathedral town of Salisbury.[1] The UK government's first task was to determine precisely what had happened to the Skripals and who was responsible. On March 12, then-Prime Minister Theresa May informed the UK Parliament of the findings of the government's investigation: "It is now clear that Mr. Skripal and his daughter were poisoned with a military-grade nerve agent of a type developed by Russia. . . . The Government has concluded that it is highly likely that Russia was responsible for the act against Sergei and Yulia Skripal." She continued ominously, "Mr Speaker, there are therefore only two plausible explanations for what happened in Salisbury on the 4th of March. Either this was a direct act by the Russian state against our country, or the Russian government lost control of this potentially catastrophically damaging nerve agent and allowed it to get into the hands of others."[2]

Although the attack was primarily a Russian assassination attempt against the traitor Skripal, it was also a chemical weapon-aided attack on the United Kingdom; when state-sponsored assassinations occur—when they are not deterred—they can dangerously weaken the stability of the countries in which they are carried out. While true with respect to assassinations, this also holds for other forms of gray zone aggression. With

Elisabeth Braw is a Resident Fellow at the American Enterprise Institute, where she focuses on defense against emerging national security challenges, such as hybrid and gray zone threats.

Interview taking place near the Maltings Police forensics tent following the attempted assassination. (Peter Curbishley, March 7, 2018)

such below-the-threshold aggression, the targeted country faces an awkward predicament: how to respond forcefully without violating the ethical standards liberal democracies have set for themselves, and more importantly, how to communicate deterrence to prevent such attacks?

Deterring Gray Zone Aggression

The primary reason gray zone aggression is an attractive option for countries seeking to increase their power at Western expense is that the West's traditional deterrence policy—based on conventional military strength and ultimately backed by nuclear weapons—has been successful in deterring traditional military aggression. Deterrence always poses a basic challenge: its effectiveness is virtually impossible to measure or prove. An absence of aggression is not a confirmation that deterrence has been successful; it may simply mean the adversary was never planning to attack in the first place. Nevertheless, nation-states have long known that they need to signal to potential attackers and the wider world that military attacks will not be tolerated and will not be successful. Some countries have projected more forceful deterrence through the course of the Westphalian world order, some less so, but all know that signaling weakness is in no country's interest.

In addition, as Hathaway and Shapiro and others such as the Uppsala Conflict Data Program have shown, armed conflict has lost significant lure among industrialized nations.[3] In this context, Russia's intervention in Crimea and Eastern Ukraine is an aberration. Geopolitical competition has, however, not vanished. The decline of inter-state war makes

gray zone aggression a convenient tool and alternative strategy for advancing standing and weakening opponents in the competitive global arena. Gray zone aggression bedevils the targeted country not just because it primarily targets civil society but because it is hard to identify, to attribute to a specific sovereign perpetrator, or both. Cyber attacks are notoriously difficult to trace to a sponsoring government, partly because no digital trail may link the perpetrators to their sponsors. Alternative forms of land acquisition as practiced by China through the gradual construction of islands in disputed South China Sea waters defy any obvious retaliatory response as no individual Chinese step seems sufficiently significant to warrant retaliation or even explicit deterrence signaling. Hostile business acquisitions by foreign entities may seem like cutthroat business as usual until a country has lost a significant number of key firms to a rival country. Crucially, because it is so difficult to establish suitable defense and response, establishing credible deterrence is a vexing challenge. What punishment or denial to signal when the nature of a prospective or even an executed attack is not even clear?

The UK government's response to the attempted assassination of the Skripals was innovative. The government quickly assembled a coalition of allies, all of which expelled Russian intelligence officers working under diplomatic cover. The United States not only expelled 60 Russians working under diplomatic cover but also ordered Russia to close its consulate in San Francisco.[4] A total of 28 countries expelled 153 Russian intelligence officers. This was not without cost to UK allies—Russia retaliated by expelling 189 individuals working in Russia on diplomatic passports.[5] The UK government also launched a communications offensive, which in combination with the muckraking efforts of investigative journalists, resulted in the two Russian perpetrators quickly being identified along with Russia's GRU military intelligence agency and shamed for their incompetence.[6]

In October 2020, soon after retiring from government service, Mark Sedwill—the UK government's national security advisor at the time of the Skripal attack—revealed that the government had struck back in other ways as well. "We also took a series of other discreet measures," Sedwill told the British newspaper *The Times*.[7] Sedwill declined to identify the discrete measures, explaining only that "we will use different techniques. We need to play to our strengths and focus our attention on their vulnerabilities. We are not going to conduct illegal operations, but there are things we can do. There are some vulnerabilities that we can exploit too." Those vulnerabilities, he said, include "tackling some of the illicit money flows out of Russia, and covert measures as well."

"Play to our strengths and focus our attention on their vulnerabilities" is a promising approach to deterrence in the gray zone. In the case of the Skripal attack, the UK actions were retaliatory, coming as they did after the attack. Successful deterrence would have signaled that such punishment would be metered out on any country attempting gray zone aggression on UK soil. UK deterrence signaling in the gray zone prior to the attack was, in fact, indisputably insufficient. The country had suffered a litany of previous gray zone aggressions including cyber attacks and even the previous successful assassination of Russian former spy Alexander Litvinenko, which also featured a toxin.

Indeed, as demonstrated by the Skripal attack, continuing cyber attacks by the governments of China, Russia, Iran, North Korea, and their proxies; coercive Chinese diplomacy; and subversive business practices, gray zone aggression persists because it is not deterred—perpetrators have been confident they can get away with impunity. Their confidence is based on the vexing difficulty of designing effective gray zone deterrence. Unlike deterring the armed forces of rival states, where countries seek to match or counter each other's military capabilities, the diversity and unpredictability of gray zone aggression leaves

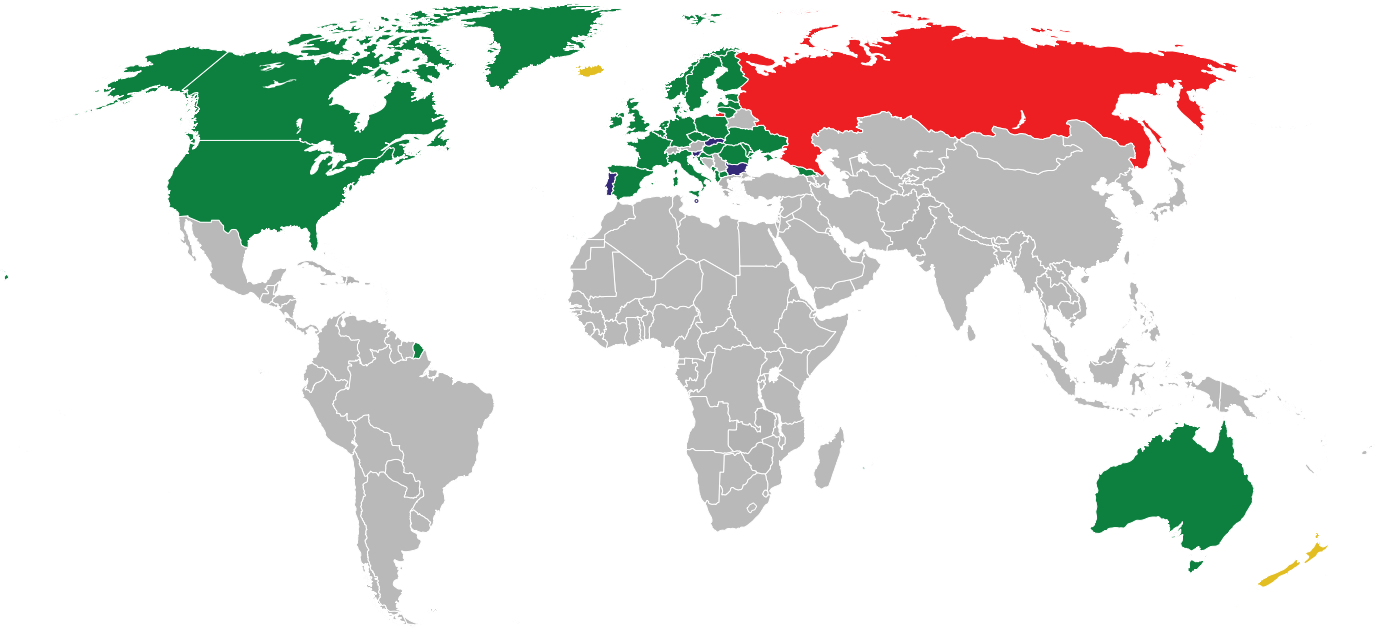
the defender one step behind. Indeed, part of the beauty of gray zone aggression is its surprise element, not only in timing but also in its methods.

The challenge presented by the diversity of methods is not only in trying to predict them but also the fact that liberal democracies are often not able to retaliate using the same methods. It would, for example, not behoove a Western country to signal that a chemical weapon-powered assassination attempt on its soil will be avenged with a corresponding assassination attempt on the adversary's soil, or that concerted use of intellectual property theft will be avenged in kind. Because the West's rivals know the ethical standards Western governments set for themselves, and that any deviation from these standards might be severely criticized by opposition parties, civil society watchdogs, and voters, deterrence that does not adhere to such standards would not be credible.

Like traditional deterrence, deterrence signaling in the gray zone must be credible. Signaling kinetic punishment for an act of gray zone aggression would be disproportionate and escalatory and thus not credible. To date, the only kinetic response to gray zone aggression has been Israel's 2019 bombing of a Hamas building in Gaza in response to a cyber attack.[8] As a result, NATO's long-serving deterrence tools, including the U.S. nuclear umbrella, are of minimal use for deterrence in the gray zone. Somewhat surprisingly, the UK government states in its Integrated Review—published in March 2021—that the UK will, in practice, seek to deter new technological threats with its nuclear arsenal. "The UK will not use, or threaten to use, nuclear weapons against any non-nuclear weapon state party to the Treaty on the Non-Proliferation of Nuclear Weapons 1968 (NPT). This assurance does not apply to any state in material breach of those non-proliferation obligations. However, we reserve the right to review this assurance if the future threat of weapons of mass destruction, such as chemical and biological capabilities, or emerging technologies that could have a comparable impact, makes it necessary." Adversaries may take this to understand that the UK will avenge devastating cyber attacks with nuclear strikes. The question is whether the adversaries will regard the threat as credible.[9]

Nevertheless, the UK government's cumulative response to the Skripal attack holds important lessons. It has almost become an article of faith that liberal democracies are powerless to deter gray zone aggression because the attacks target their vulnerable civil societies, and because they cannot avenge most attacks in kind, and thus lack punishment tools with which to deter such aggressive behavior. Russia's interference in the 2016 U.S. elections is a good case in point. The Russian disinformation campaign left many Americans convinced that their government could not protect itself against election meddling by hostile states. A September 2020 poll by the University of Chicago found that 69 percent of Americans believed Russia tried to influence the 2016 vote, while only 29 percent believed Russia did not. Fully 74 percent were concerned that foreign governments would try to tamper with voting systems or election results, and 74 percent were also concerned that foreign governments would try to influence what Americans think of their political candidates.[10]

During the 2020 U.S. election campaign, there was considerable concern that Russia would replicate its interference efforts of the 2016 election campaign. In the end, Russia's interference in the 2020 election was markedly below the level of 2016. This suggests that targeted countries are, in fact, capable of deterring gray zone aggression through resilience, punishment, or both. In the case of the 2020 U.S. elections, successful deterrence can credibly be attributed to DOD's Defend Forward offensive strategy, CISA's defense of the election infrastructure, and Americans now being on their guard against disinformation.[11] Similarly, while the UK's open borders and freedom of movement make



Poisoning of Sergei and Yulia Skripal – Countries in green expelled Russian diplomats. (Map created by Mykola Vasylechko, March 27, 2018)

it easy to attempt a government-sponsored assassination, the UK government's swift and innovative response to the Skripal attack imposed a significant cost to Russia, and thus is likely to deter similar aggression in the near future.

Liberal Democracies Fight Back

What can we learn from these recent possible examples of success? How can liberal, democratic states persuasively signal that gray zone attacks will be resisted and avenged? Western governments need to rethink deterrence. Or rather, they need to remember how successful deterrence works. The sum of deterrence by denial and by punishment aims to, in the words of Dr. Strangelove, instill in the enemy the fear to attack. It is primarily about changing an adversary's cost-benefit calculation through psychology, not specific tools. Indeed, because gray zone deterrence may require a different toolbox than that used by the adversary, the psychological factor is even more important than is the case with deterrence of traditional armed attacks. As demonstrated by the UK government's response to the Skripal incident, the West has options that are both legal and ethical. And because gray zone aggression targets civil society, societal resilience presents an enormous potential, not only as defense but also as a deterrent.

First, governments should signal that while they may not be able to prevent every attack, widespread and well-organized societal resilience means a gray zone attack will have limited impact. Such deterrence by denial was a pillar of Sweden's deterrence posture during the Cold War. While Sweden had large armed forces, with a mobilized strength of some one million, military power alone was plainly insufficient to deter the Soviet Union. Instead, deterrence relied heavily on the civil defense arm, which involved no fewer than 2.2 million Swedes,[12] who in case of an attack would maintain vital societal functions and support the armed forces, thus denying an attacker a swift victory and changing the attacker's cost-benefit calculation. Deterrence by denial—as exemplified by

the societal resilience just described—is by definition reactive. As such, it is an insufficient deterrent in and of itself. It is, however, a vital twin to deterrence by punishment as it demonstrates that even successful attacks will have relatively limited effect and will present to a prospective aggressor an unattractive cost-benefit calculation.

Second, specific retaliatory measures in the context of deterrence by punishment need not be identified in deterrence messaging. In what the author calls the "horse's-head-in-the-bed strategy," a targeted country only needs to communicate to the country sponsoring gray zone aggression that it will retaliate and impose an unacceptable cost. Deterrence by punishment should signal both to known gray zone actors such as Russia and China as well as to other countries that gray zone aggression will be avenged, and that the aggrieved state will choose the time, manner, and target to maximize effect.

Third, governments must establish who should be deterred. This is a critical departure from centuries of deterrence, where the only recipient of deterrence messaging was a rival government. Today, in the many cases where no government declares itself the perpetrator or sponsor of gray zone activities, addressing deterrence to a presumed sponsoring government is ineffective. As a result, Western governments should build targeted deterrence messaging directed at governments, government-linked companies, and individuals, respectively.

There should, in other words, be no ambiguity regarding the intention to respond to gray zone aggression and that this response will range from societal resilience to punishment of the attacker.

Putin's Palace, near the village of Praskoveevka in Krasnodar Krai, Russia. (Экологическая Вахта по Северному Кавказу, Дмитрий Шевченко, February 11, 2011)

There should, however, be ambiguity as to how the attacker will be punished, when it will be punished, and indeed which individuals or individual companies will be punished. This ambiguity is perhaps the most useful tool that Western countries can use in deterrence of gray zone aggression. It is highly beneficial for three reasons:

1. It does not lock the targeted country into responding with the same means as those used by the aggressor. This is important as the means used by the aggressor may fall outside liberal democracies' ethical norms.
2. It does not lock the targeted country into immediately responding to an attack. This is particularly beneficial as the perpetrator of a gray zone attack—whether a state or non-statal entity—can often not be immediately identified.
3. It leaves the targeted country the liberty to choose whether, when, and how to retaliate. This uncertainty itself—not knowing whether the targeted country will avenge the attack, and if it does, with which allies, and in which manner—in fact increases deterrence.

This leads to the question of which kinds of punishments liberal democracies can signal to the various targets of their deterrence. Sedwill's observation that "we need to play to our strengths and focus our attention on their vulnerabilities. We are not going to conduct illegal operations, but there are things we can do. There are some vulnerabilities that we can exploit too," is crucial. During the 2020 U.S. election campaign, presidential candidate Joe Biden referred to these vulnerabilities when he explained how he would seek to counter election interference: "I will direct the U.S. Intelligence Community to report publicly and in a timely manner on any efforts by foreign governments that have interfered, or attempted to interfere, with U.S. elections. I will direct my administration to leverage all appropriate instruments of national power and make full use of my executive authority to impose substantial and lasting costs on state perpetrators," he wrote, adding that the punishment could include "financial-sector sanctions, asset freezes, cyber responses, and the exposure of corruption."[13]

While sanctions are a much-used but not particularly effective punishment, the exposure of corruption suggests an agile approach badly needed in gray zone deterrence, and not just with regard to election meddling. Russian opposition activist Alexey Navalny's early 2021 exposé of a magnificent palace, apparently built by President Vladimir Putin through dubious means, appeared to rattle Putin more than any other allegations against him.[14] Let us not forget the resignation of Iceland's Prime Minister Sigmundur Davio Gunnlaugsson in 2016 following the release of the Panama Papers which implicated him in corrupt activities. Such exposure is clearly viewed as very threatening to corrupt leaders.

Another Russian vulnerability, shared by China and Iran, is systematic discrimination against minorities. At the time of writing, China appears to have decided that sending Uighurs to "reeducation camps" and thereby earning the opprobrium of the West is preferable to allowing the spread of Uighur separatism. Separatism is, in other words, a key concern for Beijing. Although the plight of persecuted minorities should emphatically not be leveraged in Great Power politics, Western governments could, for example, signal the possibility of intrusive examination and reporting of China's domestic conflicts and tensions. While interference in the internal affairs of other countries is decidedly a contravention of Westphalian norms and can violate international law, doing so on behalf of minorities subject to discrimination and internal to a country against their popular will is less self-evident.

Western countries also have assets their adversaries lack, and which they can employ in deterrence. The most important of these is the desirability of their countries as destinations for

visits, investment, education, or even residence. People from every country in the world want to visit or even live in the West. In countries with autocratic regimes, such as Russia and China, people with money, connections, high positions, or a combination thereof visit the West for private purposes. In many cases, their families visit Western countries with great frequency; indeed, children of such officials and businessmen often attend schools and universities in the West and stay on to work after graduation. Even after the United States and the EU imposed sanctions on, among others, Deputy Duma Speaker Sergei Zheleznyak after Russia's annexation of Crimea, his daughter Anastasia continued working as a production assistant at the BBC's prestigious Ellstree Studios. Anastasia is a graduate of Queen Mary University in London and the American School in Switzerland (TASIS), a boarding school for the moneyed global elite. North Korean ruler Kim Jong-Un also attended a Swiss boarding school.[15] Many children of top Chinese officials attend top U.S. universities, including the daughter of current Chinese leader Xi Jinping, who graduated from Harvard University in 2014. Typically, the children use assumed names.[16]

Officials and well-connected businessmen from countries hostile to the West often own property in the very countries they denigrate and sabotage. The UK Parliament's Intelligence and Security Committee noted in its Russia report—released in July 2020—that the UK has welcomed Russian money, with few questions asked about its provenance. In so doing, the Committee said that the UK "offered ideal mechanisms by which illicit finance could be recycled through what has been referred to as the London 'laundromat'. . . . Russian influence in the UK is 'the new normal'."[17] It is, however, not known to the wider public which officials from hostile countries own which properties or bank accounts in countries such as the UK. With the permission of the Western schools, universities, and employers of family members, as well as banks and property developers, Western governments can signal to perpetrators that they will reveal such facts to both their own domestic publics as well as the local community. The author refers to such public dissemination of uncomfortable facts as second-strike communications.[18] Signaling of punishment featuring such revelations could be coupled with entry bans not just for the targeted officials but for their family members as well.

To be sure, this would require cooperation from civil society entities not ordinarily involved in national security. It would also entail reaching those regimes' citizens. Chinese state authorities spare no effort to prevent such access by banning Western social media platforms such as Twitter. Nevertheless, many ingenious Chinese citizens do manage to access proscribed content. While Russians—often with justification—distrust Western criticism of their government, exposés of officials' families living large in the West on taxpayer money could cause a stir. Neither Western banks nor universities would delight in cooperating with their home governments in exposing some of their well-paying customers. The issue of Chinese and Russian influence in the West is, however, gaining so much attention in the public debate that both educational institutions and commercial firms may be convinced to do so, if only to cleanse their brands.

In response to, say, a new case of systematic intellectual property theft by companies linked to the Chinese government, one possible response might be to draw attention to the U.S. university enrollment of certain Chinese officials' children. Better yet, it should signal that such revelations may be part of the punishment. This should not be a general accusation—if nobody is named, nobody will be shamed—but signaling that specific individuals, officials, and their families will be singled out.

Traditionally, Western governments have not highlighted foreign leaders' private associations

Justice Department charges five Chinese members of APT41 over cyberattacks on U.S. companies. (Federal Bureau of Investigation, September 19, 2020)

with their countries, as it seemed irrelevant to Great Power politics and was at any rate considered contrary to diplomatic protocol. With hostile governments hiding behind gray zone acts to weaken the West it is, however, imperative that Western governments be more innovative and daring, while yet adhering to their ethical standards. Indeed, if Western governments demonstrate an ability to think creatively about retaliation, they will constantly keep the attackers in uncertainty and fear, thereby reducing the country's appetite for aggression. As Thomas Schelling reminded policymakers, surprise is a key element of deterrence.[19]

There is precedent in communicating with rivals' publics. During the Cold War, governments on both sides established radio stations serving the populations of their rival states. Radio Free Europe/Radio Liberty, initially funded by the CIA, was part of that effort.[20] Of course, if Western governments increase their already existing efforts to communicate with rivals' citizens, they cannot criticize rival governments for communicating with theirs.

Retaliation could, as Biden suggested, also include publicly sharing information about corruption. In addition, it should clearly include Defending Forward and its sister policy, criminal indictments against individual perpetrators. The Trump administration continued its predecessor's nascent practice of not just naming and shaming countries to which it had attributed cyber attacks, but of indicting individual perpetrators as well. On September 16, 2020, the Department of Justice charged five Chinese nationals with cyber attacks on more than 100 companies in the United States and elsewhere;[21] one month later it charged six officers in Russia's military intelligence agency with cyber attacks against Ukraine, Georgia, the 2017 French election campaign, and the 2018 Winter Olympics.[22] The officers were also charged with having perpetrated the devastating NotPetya attack in 2017, which was directed against Ukraine but brought down a range of international companies as well. In July 2020, the EU issued its first-ever sanctions over a cyber attack, imposing a travel ban and other penalties on six Russian and Chinese nationals involved in NotPetya and several other attacks.[23]

Criminal prosecutions constitute an even stronger deterrent but are only possible if the defendant is present; and a targeted foreign official is highly unlikely to present him- or herself for prosecution abroad. Because indictments, however, effectively bar the accused from entering the country (for reasons other than presenting him- or herself to law enforcement authorities), and subject them to possible extradition to the United States if apprehended in third countries, they block an attacker from benefits available to the general public. The attacker thus has to weigh participating in gray zone aggression on behalf of a government against being able to travel freely abroad or visit the United States.

These examples illustrate some of the possibilities of targeted deterrence. The author refers to the this as *personalized deterrence*.[24] Its basic operating assumption is that many officials and other perpetrators and sponsors of gray zone aggression are likely to be more loyal to themselves than to their regimes, and that the prospect that they will personally suffer retaliation by the United States can substantially change their cost-benefit calculation. The objective—following Schelling's surprise element dictum—is to keep representatives of the hostile country guessing as to which punishment will be meted out, whom it will target, and when—and whether—it will take place.

As with deterrence by punishment, deterrence by denial should be demonstrated and thereby communicated to countries already engaged in gray zone aggression and countries flirting with the prospect. Military exercises do not just serve the purpose of soldiers perfecting their skills but the equally important message of signaling those skills to potential attackers. Specially designed exercises can also be used to signal to would-be adversaries that their efforts to subvert our interests through gray zone aggression will yield insufficient gains to justify the costs. To date, although government agencies have practiced for contingencies related to gray zone aggression, there have been no specific gray zone defense exercises. The closest existing exercise is Sweden's *Total Defense 2020* exercise, which focuses on traditional threats but does include all parts of the government as well as businesses and volunteers. During the Cold War, Sweden regularly held total defense exercises; this exercise is the first such since 1987.[25] Given the nature of gray zone aggression, such exercises should involve the armed forces, the government, industry, and civil society volunteers, and be of a purely defensive nature.

The author has proposed a concept for gray zone exercises involving the armed forces, industry, and other relevant government agencies. The government would identify private companies that would benefit from gray zone preparation; that is, most companies engaged in critical national

infrastructure in the wider sense. Businesses would also be able to apply to participate. Upon conclusion of the exercises, participating businesses would be awarded ISO-style certification, which they could keep current through renewed participation in gray zone exercises.[26] In January 2021, the Czech Republic premiered the concept with a pilot exercise.[27]

In the six years since Russia's annexation of Crimea—the event generally considered the West's wakeup call concerning Russia's ability to use gray zone aggression—the focus has been on Western vulnerabilities in the face of their adversaries. There is no doubt that the open borders and free societies characteristic of liberal democracies that allow citizens and foreigners alike to pursue their lives unimpeded by government present countless opportunities for gray zone aggression by unscrupulous adversaries. By thinking innovatively, however, Western countries can improve both their deterrence by resilience and deterrence by punishment to at least discourage if not prevent gray zone aggression. By creatively using their advantages, Western countries in cooperation with their allies can mitigate their vulnerabilities. Indeed, innovative thinking is a deterrent in itself, one that keeps the attacker uncertain about the resilience and punishment that might ensue, and thus changes the cost-benefit calculus. PRISM

Notes

[1] "Russian spy poisoning: What we know so far," BBC, October 8, 2018, available at <https://www.bbc.co.uk/news/uk-43315636>.

[2] Prime Minister Theresa May, "Oral statement to Parliament: PM Commons statement on Salisbury incident," March 12, 2018, available at <https://www.gov.uk/government/speeches/pm-commons-statement-on-salisbury-incident-12-march-2018>.

[3] Oona A. Hathaway and Scott J. Shapiro, *The Internationalists: How a Radical Plan to Outlaw War Remade the World* (New York: Simon and Schuster, 2018). For figures since 1946, see, Uppsala Conflict Data Program, "Armed Conflicts by Region and Year, 1946–2019," available at <https://ucdp.uu.se/downloads/charts/>.

[4] Julian Borger, "US orders Russia to close consulate and annexes in diplomatic reprisal," *The Guardian,* August 31, 2017, available at <https://www.theguardian.com/us-news/2017/aug/31/us-russia-san-francisco-consulate-close>.

[5] Alia Chughtai and Mariya Petkova, "Skripal case diplomatic expulsions in numbers," Al Jazeera, April 3, 2018, available at <https://www.aljazeera.com/news/2018/4/3/skripal-case-diplomatic-expulsions-in-numbers>.

[6] Elisabeth Braw, "Second Strike Communications," *Royal United Services Institute (RUSI) Newsbrief* 39, no. 4 (May 17, 2019), available at <https://rusi.org/publication/rusi-newsbrief/second-strike-communications>.

[7] Tom Newton Dunn and Mark Sedwill, "We always hit back hard. Russia paid a high price for Salisbury poisonings," *The Times*, October 24, 2020, available at <https://www.thetimes.co.uk/edition/news/mark-sedwill-we-always-hit-back-hard-russia-paid-a-high-price-for-salisbury-poisonings-5v3n3hngk>.

[8] Zak Doffman, "Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First," *Forbes,* May 6, 2019, available at <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=3209e8caafb5>.

[9] *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, presented to Parliament by the Prime Minister by Command of Her Majesty, March 2021, 77, available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf>.

[10] *Americans Split on Relationship with Russia*, University of Chicago Harris School of Public Policy and The Associated Press-NORC Center for Public Affairs Research, September 11–14, 2020, available at <https://apnorc.org/wp-content/uploads/2020/10/topline_release1.pdf>.

[11] Elisabeth Braw, "This Time, the Meddling Is Coming From Inside the House," *Foreign Policy,* November 5, 2020, available at <https://foreignpolicy.com/2020/11/05/election-hacking-domestic-trump-biden-vote/>.

[12] Försvarshögskolan, *Förutsättningar för krisberedskap och totalförsvar i Sverige* (2019), 19, available at <https://www.fhs.se/download/18.165b2e611685dbe45333940a/1549227413452/F%C3%B6ruts%C3%A4ttningar%20f%C3%B6r%20krisberedskap%20och%20totalf%C3%B6rsvar%20i%20Sverige%202019.pdf>.

[13] John Verhovek, "Biden warns against foreign interference in US elections: 'I am putting the Kremlin and other foreign governments on notice'," ABC, July 21, 2020, available at <https://abcnews.go.com/Politics/biden-warns-foreign-interference-us-elections-putting-kremlin/story?id=71886014>.

[14] "Vladimir Putin: Russian palace in Navalny video not mine," BBC, January 25, 2021, available at <https://www.bbc.co.uk/news/world-europe-55799143>.

[15] Elisabeth Braw, Educating Their Children Abroad Is the Russian Elite's Guilty Secret, *Newsweek,* July 30, 2020, available at <https://www.newsweek.com/2014/08/08/educating-their-children-abroad-russian-elites-guilty-secret-261909.html>; see also "Tuition and fees," The American School in Switzerland, available at <https://www.tasis.ch/page.cfm?p=736>.

[16] Andrew Higgins and Maureen Fan, "Chinese communist leaders denounce U.S. values but send children to U.S. colleges," *Washington Post,* May 19, 2012, available at <https://www.washingtonpost.com/world/asia_pacific/chinese-communist-leaders-denounce-us-values-but-send-children-to-us-colleges/2012/05/18/gIQAiEidZU_story.html>.

[17] Intelligence and Security Committee of Parliament, *Russia Report*, presented to Parliament Pursuant to Section 3 of the Justice and Security Act of 2013, July 21, 2020, available at <https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl>.

[18] Braw, "Second Strike Communications," May 17, 2019.

[19] T. C. Schelling, *The Reciprocal Fear of Surprise Attack* (Santa Monica, CA: RAND, April 16, 1958), available at <https://www.rand.org/content/dam/rand/pubs/papers/2007/P1342.pdf>.

[20] "History," Radio Free Europe/Radio Liberty, available at <https://pressroom.rferl.org/history>.

[21] Department of Justice, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," press release, September 16, 2020, available at <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>.

[22] Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, October 19, 2020, available at <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.

[23] Lorne Cook, "First ever EU cyber sanctions hit Russian, Chinese, NKoreans," AP, July 30, 2020, available at <https://apnews.com/article/malware-technology-foreign-policy-international-news-military-intelligence-978f1494313a545e6e7e568e5f9782bf>.

[24] Elisabeth Braw and Gary Brown, "Personalised Deterrence of Cyber Aggression," *The RUSI Journal* 165, no. 2 (March 18, 2020), 48–54.

[25] *Försvarsmakten/MSB*, Totalförsvarsövning 2020. Tillsammans försvarar vi Sverige, <https://www.forsvarsmakten.se/contentassets/dd56a6422b8e496ab552c5f4186da291/tfo_faktablad_se-faststalld.pdf>; see also, Gerhard Wheeler, "Northern Composure: Initial Observations from Sweden's Total Defence 2020 Exercise," RUSI, September 3, 2020, available at <https://rusi.org/commentary/northern-composure-initial-observations-swedens-total-defence-2020-exercise>.

[26] Elisabeth Braw, "The Case for Joint Military–Industry Greyzone Exercises," *RUSI Briefing Papers*, September 28, 2020," available at <https://rusieurope.eu/publication/briefing-papers/joint-military-industry-greyzone-exercises>.

[27] Helen Warrell, "Czech Republic turns to war-games to build cyber defences," *Financial Times,* February 17, 2021. <https://www.ft.com/content/8c018644-3866-4f69-9105-d3c0e68ca491>.

STRATEGIC LANDPOWER SYMPOSIUM

REGISTRATION AND CALL FOR PAPERS

10-12 MAY 2022
US ARMY HERITAGE EDUCATION CENTER
CARLISLE, PA

The **USAWC** in partnership with **HQDA G3/5/7** are pleased to announce the first annual Strategic Landpower Symposium (SLS), to solicit research and encourage professional discussion on "Strategic Landpower in Cooperation and Competition."
(see Chief of Staff Paper #1)

Papers should consider:
The Future Role of Strategic Landpower in Integrated Deterrence; Cooperation; Competition; and/or, Joint All Domain Operations.

Submissions on related topics are also welcome.
Call for papers submission deadline is 1 December 2021.

See website for details:
https://csl.armywarcollege.edu/landpower/

Dr. Greg Cantwell
email: gregory.l.cantwell.civ@mail.mil
THE UNITED STATES ARMY WAR COLLEGE