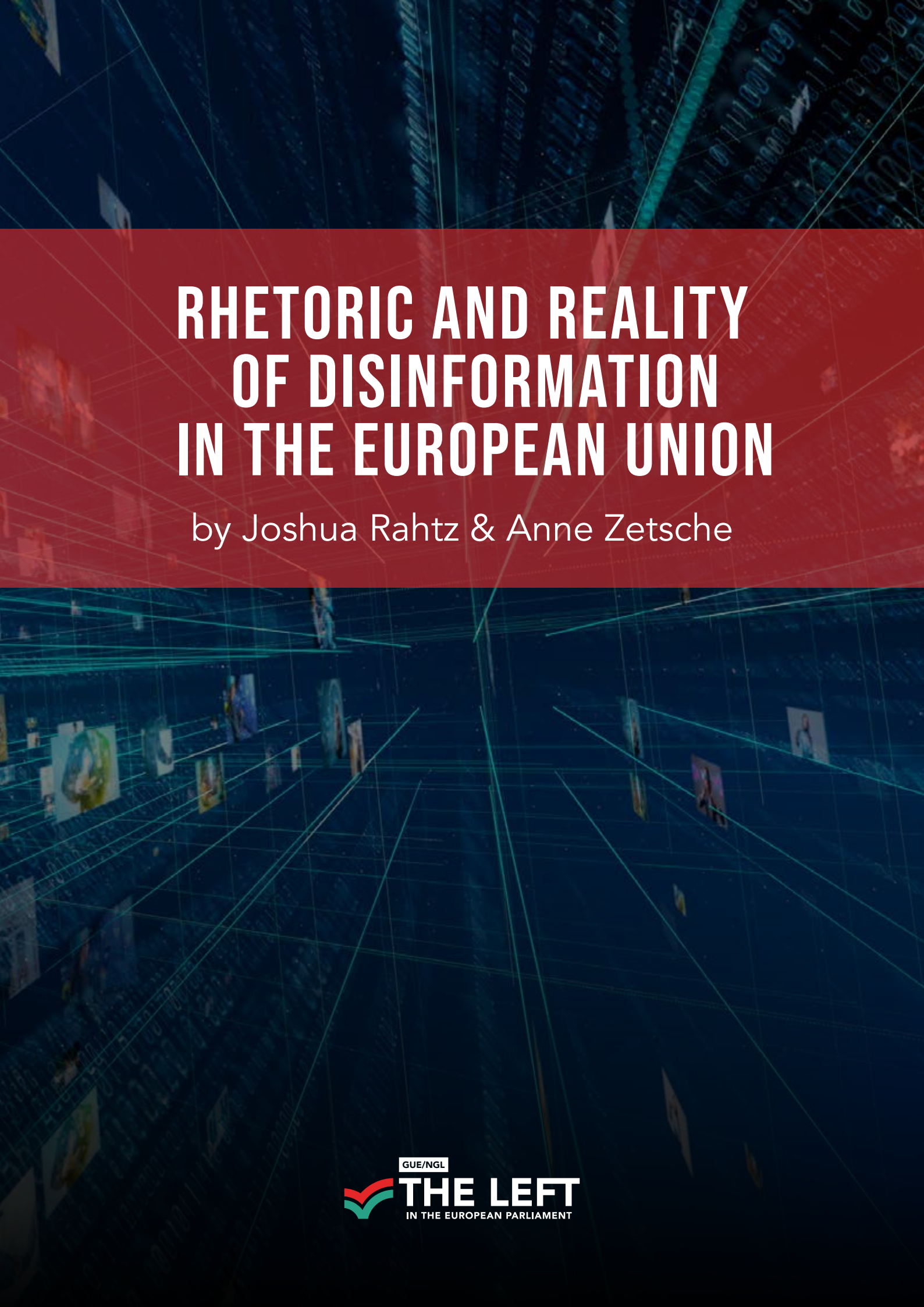

RHETORIC AND REALITY OF DISINFORMATION IN THE EUROPEAN UNION

by Joshua Rahtz & Anne Zetsche

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

Rhetoric and Reality of Disinformation in the European Union

by Joshua Rahtz & Anne Zetsche

Study for The Left in the European Parliament

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

B-1047 Brussels, Belgium
+32 (0)2 283 23 01
left-communications@europarl.europa.eu
www.left.eu

July 2021

About the authors:

Anne Zetsche received her doctoral degree in history from Northumbria University, UK and works as an independent researcher and author. In September 2021, she was elected to the municipal council in Berlin Charlottenburg-Wilmersdorf for DIE LINKE.

Joshua Rahtz holds a PhD in history from UCLA and works as an editor and translator in Germany.

FOREWORD

In 2020, the European Parliament created a Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE). The committee's creation confirmed the arrival into the European political mainstream of the "foreign interference" narrative, which has been gaining traction in the European and American political and press establishments over the last six years. It is our experience from sitting on this Special Committee over recent months that its work is directed towards bolstering the "foreign interference" narrative, and it is our prediction that its final report, due in 2022, will signal the endorsement by the mainstream European political groups of the essential elements of this narrative.

"Foreign interference" is a narrative of blameless European victimhood at the hands of malign foreign adversaries who, moving among the shadows, have succeeded in interfering with and subverting European democracy. The primary antagonists in the "foreign interference" narrative are Russia and China. The principal methods of this supposed interference are unconventional: rather than using secret agents or ordinary weapons, foreign adversaries are believed to be propagating information calculated to sow alien divisions in European society, to undermine public trust in European institutions, and to skew the results of democratic elections.

By virtue of its open and democratic values and its respect for freedom of expression, Europe is presented as particularly vulnerable to interference of this nature. "Foreign interference" has, as a result, come to be understood as an exotic new form of warfare, in which information, ideas and arguments circulating in the public sphere - especially those that challenge mainstream political narratives - are no longer mere currency in the marketplace of ideas, but potential threats to national security, and must therefore be treated with suspicion, and restricted if necessary.

The "foreign interference" narrative has become established in the European mainstream on the basis of very little evidence. Most allegations of foreign interference are difficult to either prove or falsify, and rely on conspiratorial suspicion or runaway confirmation bias. Where it can be substantiated that information manipulation has taken place, it is notoriously difficult to attribute it to any specific actor, or to establish that it had any effect. In the most sensationalised cases of alleged foreign interference - such as the alleged Russian interference in the 2016 election in the United States, or the Brexit referendum in the UK - subsequent investigations have either failed to substantiate that foreign interference actually occurred, or failed to establish that genuinely malign activity on the part of foreign actors had any actual effect on electoral outcomes.[1] Despite this, because of wholesale acceptance of these narratives by the mainstream press, the myths of consequential Russian or Chinese interference in Western elections enjoy acceptance across much of the political spectrum, and are immune to contradictory evidence.

Protecting democratic processes from any kind of interference is an important task in a democratic society, but the INGE Special Committee is so selective in its focus as to make it incapable of performing this role. The main threat to the integrity of democratic processes is not foreign, but comes from wealthy and powerful interests interfering in the political process through corruption, corporate

1 See for example "UK probe finds no evidence that Cambridge Analytica misused data to influence Brexit," Politico, https://www.politico.eu/article/no-evidence-that-cambridge-analytica-misused-data-to-influence-brexit-report/ and "The end of Russiagate," Le Monde diplomatique https://mondediplo.com/2019/05/02russiagate-en

lobbying, political funding, elite capture, think-tanks and institutes, and through ownership of mass media.[2] These forms of interference - which are largely acceptable to the European political mainstream - are omitted by the Special Committee's exclusive focus on "foreign" interference.

It is also the case that over the last several centuries the phenomenon of interference in democratic processes has usually involved European and North American countries interfering in the internal affairs of countries in the Global South. Even today, we can see many examples of how the European Union, through its strategic communication, its European External Action Service and other tools and mechanisms at its disposal, tries to maximise its impact and influence in third countries. These examples are excluded from the INGE Special Committee, because its mandate exclusively focuses on alleged interference in European democracies. The resulting lack of any acknowledgement, let alone examination, of the history of European and North American interference gives rise to a dangerously skewed understanding of foreign interference as a novel phenomenon, uniquely suffered by Western states at the hands of official enemies.

Despite its official purpose, the Special Committee does not therefore have the protection of democratic processes as its primary aim. Why then has the mantra of "foreign interference" so forcefully emerged into the European political arena? Our view is that the narrative is politically convenient for the European political mainstream, and that it fulfils several political purposes at once.

In the abstract, the belief that European society is being subverted and undermined by foreign adversaries is a form of denialism about the true causes of the EU's own internal crisis. European publics are disenchanted with the neoliberal ideology that has been dominant over recent decades, during which the social democratic state has been further dismantled, and income and living standards have declined. Our societies have seen increasing polarisation, and a significant decline in support for traditional mainstream political parties, leading to the widely observed "shrinking of the centre ground." Rather than confronting changing realities and engaging in political renewal, the spectre of "foreign interference" offers European establishment parties a convenient foreign scapegoat for their own failings. It is obvious that China, the United States, Russia, and other major geopolitical actors defend their own interests globally, but the obsession with Russian and Chinese meddling in the affairs of the West can be understood as a morbid response to the diminishing political legitimacy of the neoliberal project in Europe.

The narrative of "foreign interference" has also proven useful to the European establishment as a means of marginalising political opposition and advancing a regime of stealth censorship, especially on matters of foreign policy. According to the logic of the European political mainstream, any critique of EU foreign policy which bears a resemblance to that of its chosen adversaries can be considered illegitimate, if not itself an attack on European democracy. This has allowed the mainstream political groups to insinuate that foreign policy positions advanced by the Left in the European Parliament, such as promoting military neutrality, anti-imperialism, peace and diplomacy, are aiding foreign powers. Furthermore, benign links with sovereign countries, such as diplomatic contacts, language schools or cultural exchanges, are reimagined as vectors of foreign interference, and treated as security threats. This has led to concerning attempts in the INGE Special Committee to shrink the space for alternative media and civil society, laying the ground for censorship of social media and the use of sanctions against critical outlets and organisations. We have seen this in attempts from right wing political groups to ban certain Russian-based media outlets in the EU.

2 According to a major poll conducted by the European Council on Foreign Relations, a majority of Europeans concur in the belief that the private sector has more influence over the functioning of their societies than foreign governments. Asked "Which of these groups has the most impact on the way the world is run?", 22% of those polled chose "Multinational companies," while 21% chose "Legitimate national governments and parliaments working together." A further 16% chose "Billionaires such as Bill Gates, George Soros, Charles Koch and Mark Zuckerberg," and 14% chose "A hidden network of global elites." The Chinese government ranked 6th, with 6% of those polled, behind the US government at 5th place, with 13% of those polled. https://ecfr.eu/publication/what-europeans-think-about-the-us-china-cold-war/

A third function of the "foreign interference" narrative is how it folds into the foreign and security policy agenda of the large European groups, who support the project of European defence integration, desire a more expansionist foreign policy and have identified Russia and China as their antagonists of choice. The discourse on "foreign interference" is a convenient source of imagined threats to European security, which can serve to justify new defence projects and initiatives, and drive more funding towards the security and defence sectors. A burgeoning industry in NATO-affiliated think tanks and institutes has emerged to feed into the "foreign interference" policy agenda, regularly invited to hearings of the Special Committee to provide made-to-measure expertise. It is this conglomerate of think tanks and institutes, which exist to certify the EU establishment's foreign and security policy agenda, that is the focus of this study.

As members from The Left in the European Parliament, we are struggling in the opposite direction, to achieve a model of international relations based not on confrontation, but on peace and collaboration, and for an approach to global security which takes into account the real challenges of our century, such as worsening inequality, threats to global health and the climate crisis, rather than promoting arms races with our neighbours.

The MEPs of The Left
in the INGE Special Committee

TABLE OF CONTENTS

INTRODUCTION

Across NATO member countries, the concept of disinformation now passes without critical scrutiny as a favored explanation for mounting political distemper.[1] Linked to the ostensible intrusion of foreign powers, especially Russia and China, little by way of self-reflection accompanies the category and the reality of its instrumental use – as rhetoric, but also as part of the West's offensive battery against its professed strategic rivals. Broad use of the term has selected for ambiguity and innuendo, rather than clarity. Above all, the chatter about disinformation pouring in from abroad has recast normal diplomacy, let alone more unorthodox public relations efforts outside official channels, as security threats to be met through stepped-up militarization of European societies, for which the latest in surveillance, artificial intelligence and cyber technology will be deployed. For the societies of Europe, "disinformation" and "foreign interference" will mean higher military expenditure, directly in the form of traditional budgets, where a two per cent of GDP threshold is considered a minimum, and indirectly, through the use of public-private partnerships in areas with military applications. In the context of the current acute slowdown of the European economy, after more than a decade of weak recovery dating from 2008-10 and amid a prolonged deterioration of global economic dynamism, the ratio of military to non-military expenditure has already grown dramatically. It will rise even further should such programs be realized.[2]

No government can afford to ignore the changing modes of communication which have fragmented the public sphere globally. China and other members of the BRICs (Brazil, Russia, India) in particular may be expected to attempt to keep pace with the United States, Europe and Japan in the development of their own think tanks and media. This dynamic is reflected in the composition of the *Global Go To Think Tank Index and Ranking*, published since the late 2000s, and which outside the United States has in the recent period attracted the strongest academic and media attention in these countries.[3] Unsurprisingly, Russia, China and Iran, which are frequently singled out and blamed unilaterally for "foreign interference," will naturally expand their communications in Europe and elsewhere to counter actions detrimental to their interests. Yet, irrespective of the course of intensified public diplomacy, the last quarter century of US-NATO militarism and the increased prominence of private interests in international relations requires more sober analysis.

To this end, the present report documents empirically the use of disinformation at rhetorical and operational registers whose origins and motivations are internal to the NATO alliance itself.[4] Where they originate from outside the societies of the European Union, the instances of foreign interference of greatest consequence will be shown to have sprung from the United States, which to this day enjoys unparalleled global military supremacy. In its European domain alone, it billets 70,000 troops permanently across military bases in EU member states, from which it commands global operations, including in the last two decades covert programs of torture and mass surveillance, with EU citizens among their targets.[5] The EU is headquarters not only of the US European, but also its African Command, and EU territory has been a critical transit point for US special operators shuttling between undeclared war zones. The US's National Security Agency (NSA) has monitored senior EU officials over the course of its economic crisis and beyond, and was, already in 1998, the subject of a European Parliament report on industrial espionage

1 See for example, "G7 to look at rapid response mechanism against Russian 'propaganda', UK's Raab says," *Reuters*, 2 May, 2021, in which it is reported that "Russia and China are trying to sow mistrust across the West...according to British, U.S. and European security officials." For a parallel story in the German press, see "EU wirft Russland und China Fake-News-Kampagnen vor," *Süddeutsche Zeitung*, 26 April 2020.

2 Diego Lopes Da Silva et al., "Trends in World Military Expenditure 2020," Stockholm International Peace Research Institute (April 2021), pp. 8-9 (https://sipri.org/sites/default/files/2021-04/fs_2104_milex_0.pdf).

3 A detailed overview of this think tank ranking and its perception in media and academia has been provided in a series of four blogposts, the first of which may be found here: http://thinktanknetworkresearch.net/blog_ttni_en/understanding-the-global-go-to-think-tank-index-part-1/

4 It is to be assumed that nearly all states, allies and adversaries alike, maintain intelligence and counter-intelligence operations against one another, including efforts at influencing public opinion. For a glimpse of such ongoing activity, see "Pakistan accuses India of funding disinformation campaign in EU," *Reuters* 12 December, 2020.

5 For discussion of the CIA's kidnapping of German citizen Khaled El-Masri, set in the wider context of its programs across Europe, see: "CIA-'Extraordinary Rendition' Flights, Torture and Accountability – A European Approach," European Center for Constitutional and Human Rights (Berlin: 2009).

and other surveillance, fifteen years before Edward Snowden's revelations.[6] In this context, the rhetoric of disinformation may be understood as one asset of this security regime. It is a technique of cover and deception for an agenda of threat inflation, and is driven by NATO's own bureaucratic imperatives and US-American strategic considerations vis-à-vis the Eurasian landmass.

Within EU foreign policy circles, and reflected in their use by the INGE Special Committee, the terms "foreign interference" and "disinformation" are determined by definite priorities which nevertheless remain opaque. It is therefore essential to articulate the NATO agenda driving the discussion of these factors. The extent to which NATO itself constitutes an unspoken form of influence over the EU must also be underscored. Historically, the EU and NATO are tightly linked, and it is not customary to regard the *de facto* US leadership of NATO as a potentially foreign influence in European societies.[7] Nevertheless, it is the case today that US foreign policy, with EU collaboration, threatens ramped-up militarization, an increase in the risk of large-scale conflagration and the introduction of the many corrosive effects of large militaries, such as their environmental destructiveness and diversion of wealth away from progressive reforms.[8]

In an early working document presented at INGE, the committee's rapporteur has detailed the forms and aims of alleged foreign interference within the European Union. In the report, only China, Russia and Iran are mentioned as "particularly active in this field," and they are accused of having undertaken their interference in order to "weaken, divide, or discredit the EU."[9] Although Russian and Chinese interference in EU affairs remains unsubstantiated, the rapporteur states as fact that "Russia, China, and other authoritarian regimes have funneled more than $300 million into 33 countries… half of these cases concern Russia actions in Europe."[10] The document, which rehearses much of the stereotyped banalities about eastern adversaries, highlights especially the threat of so-called hybrid warfare.

A striking feature of INGE's agenda is the prominence of Atlantic-oriented think tanks such as the German Marshall Fund, official NATO representatives and companies contracting with the US military, like Google. These links are not incidental. The CIA's venture capital arm In-Q-Tel was an early investor in Google,[11] and the company's erstwhile CEO Eric Schmidt was in 2016 the inaugural chairman of the Defense Innovation Advisory Board, a body set up to advise the Pentagon on the military uses of digital and other computing technologies. The Krebs-Stamos Group, founded in early 2021 by the former director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Christopher Krebs, and former chief of security for Facebook Alex Stamos, now consults in cybersecurity for private clients.[12] A month after Krebs delivered the keynote speech to the European Online Seminar titled "The disinformation dilemma: How to respond and regulate without undermining democracy?"

6 The NSA's Echelon was a joint US-UK communications-intelligence operation, first uncovered by an internal European Parliament report of January 1998 titled "An Appraisal of Technologies for Political Control." For an overview of this history, see the 2014 report by the Parliament's historical archives unit: Franco Piodi and Iolanda Mombelli, "The ECHELON Affair" (Luxembourg: 2014). For more recent instances, see "The NSA's Secret Spy Hub in Berlin," *Der Spiegel*, 27 October, 2013. The NSA was revealed by Edward Snowden to have tapped Merkel's cell phone

7 This was most dramatically illustrated by the divisions emerging within the West in the lead-up to the US-UK attack on Iraq in 2003. NATO was however quick to provide military advisers to the Iraq campaign as soon as 2004, which it extended through 2011, and in 2018 renewed, down to the present. In its 1999 air war on Yugoslavia, NATO as such did not flinch from violating the UN charter, and its EU members have never meaningfully obstructed US operations.

8 See for example Benjamin Neimark, Oliver Belcher, Patrick Bigger, "US military is a bigger polluter than as many as 140 countries – shrinking this war machine is a must," *The Conversation* 24 June, 2019, and "The US Department of Defense Is One of the World's Biggest Polluters," *Newsweek*, 17 July, 2014 (https://www.newsweek.com/2014/07/25/us-department-defence-one-worlds-biggest-polluters-259456 and https://theconversation.com/us-military-is-a-bigger-polluter-than-as-many-as-140-countries-shrinking-this-war-machine-is-a-must-119269).

9 The report states only that this figure is arrived at "according to findings shared with our committee" – by whom or by what it is not clear. See Sandra Kalniete, "Working Document on Foreign Interference in all Democratic Processes in the European Union, including Disinformation," 17 December, 2020, p. 3. (https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/INGE/DT/2021/01-11/1220809EN.pdf).

10 Ibid., p. 6

11 "The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows," *Wall Street Journal*, 30. August 2016 and "Google, CIA, Invest in 'Future' of Web Monitoring," *Wired*, 28 July, 2018

12 "Former Google CEO Schmidt to head new Pentagon innovation board," *Reuters*, 12 March, 2016; "Chris Krebs and Alex Stamos have started a cyber consulting firm," *Tech Crunch*, 8 January, 2021.

Stamos was invited to INGE's public hearing on "Tech Developments and Regulatory Approaches regarding Disinformation."[13] Krebs has recently pushed the US to escalate measures against ransomware attacks, and has advocated the use of the military for this purpose.[14]

In line with these developments, NATO's European think tanks aim to shape public opinion and political decision-making within EU institutions. They amplify and repeat NATO priorities, advance US strategic interests, and in so doing drive military funding. Such activity indicates the degree to which the current social crisis across European societies is mystified by elements internal to the EU's military and military-intelligence alliances. It is the perspective of this report that the prevailing definition of enemies and adversaries does not serve the interests of the populations of Europe, but rather those of the US's foreign policy coalition (including its European counterparts), its strategists and the US and European firms linked to it which profit immensely from perpetual emergency[15]

*

The present study of US and NATO influence within the EU is divided into two parts.

Part I provides an overview of the geopolitical context and the expansion of the concept of security which has served to legitimize NATO's continued existence since the collapse of the Soviet Union. The alliance's enlarged domain has grown to include new fields such as the environment, human rights and civil society. Yet the period has also been characterized by the expansion of conventional US and NATO wars. A study of the relation of these terms will be the focus of Part I's analysis of the Iraq war and its lead-up.

Part II examines three NATO think tanks based in central and eastern Europe. In transforming itself from an alliance focused exclusively on interstate warfare into an international military body capable of global operations, NATO founded a network of security think tanks to develop new concepts and doctrines that would cover its extended portfolio. Two of those discussed below are components of the so-called NATO Centers of Excellence, each of which in its respective field illustrates well the expansion of the concept of security across the realms of cyberspace and communications. The Tallinn-based Cooperative Cyber Defence Centre of Excellence demonstrates clearly how under the pretext of defensive exercises in cyber warfare[16] NATO has transformed the internet from a civil technology into yet another area of armed conflict. As NATO and the EU make joint preparations for intensified hostilities with Russia and China, they must also establish public acquiescence to NATO operations, within and outside of their own members' societies. This is the concern of Riga's Strategic Communications Centre of Excellence, which specializes in psychological and information warfare and public relations. Last, and independent of Centers of Excellence, is the NATO and the US State Department-funded think tank GLOBSEC. Based in Bratislava, it serves as a networking hub in the East which consolidates the Atlantic orientation of central and eastern European capital and officialdom, and prepares NATO for further eastward expansion. Taken together, these three organizations exemplify NATO's current orientation and the centrality to it of public diplomacy and information warfare.

13 INGE draft agenda to joint meeting, 15 April, 2021: https://www.europarl.europa.eu/doceo/document/INGE-OJ-2021-04-15-1_EN.html

14 "Former US cyber chief calls for military to attack hackers," *Financial Times*, 5 February, 2021.

15 On the power and influence of the European arms industry and lobby, especially in defining security and defense policies, see Jordi Calvo Rufanges, "The Arms Industry Lobby in Europe," *American Behavioral Scientist*, 2016, 60 (3): 305-320.

16 The term here refers to multiple applications of digital and internet-based war, including espionage, propaganda and sabotage of infrastructure, all undertaken with "plausible deniability." See Kenneth Geers, *Cyberspace and the Changing Nature of Warfare* (Tallinn: CCDCOE, 2008): https://ccdcoe.org/library/publications/cyberspace-and-the-changing-nature-of-warfare/

01

THE SECURITY STATE

GEOPOLITICS AFTER THE COLD WAR

From the vantage of the US foreign policy establishment, Eurasia – the continent extending from Lisbon to Vladivostok – has long been understood as the definitive zone of world politics. Surveying the post-Cold War scene in 1997, the realist US national security adviser Zbigniew Brzezinski characterized it as "the chief geopolitical prize,"[17] and the field on which potential emerging rivalries with China and Russia would naturally be decided. Europe's geostrategic importance would remain central to its development, among other reasons because at its western extremity lay the "key and dynamic geostrategic players" of France and Germany.[18] Yet by 2012, Brzezinski warned that the US risked a "dispersal" of its power, as a passive Europe – the US's key strategic outpost and partner in a unique "American-dominated West" – had become more internally fractured, and therefore threatened the order built around NATO's Atlantic agreements, leaving the US "increasingly...with the ultimate responsibility for Europe's security."[19] Here, according to Brzezinski, the temptation of Russian energy wealth pulled Germany into Moscow's orbit; this fact was made more diplomatically treacherous given the failure of full integration of Russia into the West after 1991, thus spoiling a consolidation of a "larger West" which might encircle a rising China and ensure global "stability." In its recklessness following the turn of the millennium, the US had only detonated greater disorder, and had set itself and the West back.[20]

In a 2018 book-length essay, the neo-conservative strategist Robert Kagan likewise lamented the passivity of European powers in taking on rising geostrategic competitors of both Russia and China. Russia, for Kagan, now conforms "to the long sweep" of its history, by rejecting integration into the American-led liberal international order and opting for a "return...to its historical influence on the world stage" at its expense.[21] China, for its part, according to Kagan, has experienced a renewed nationalism, dispensed with Deng's maxim to keep a low profile, and is now "returning to old visions of hegemony."[22] For Kagan, the capstone achievement of George H.W. Bush and Helmut Kohl was having brought a newly unified and appropriately constrained Germany into NATO; the latter, along with the EU, has been the key to Europe's peaceful stability. These diplomatic conditions succeeded in breaking with the centuries-long history of European enmity. But Kohl and Bush's triumph is now threatened, so Kagan argued, as nationalist populism has returned to the Continent, expressing itself above all as opposition to the EU and NATO and attendant sympathy with Russia.[23] In part, for Kagan, this was the "price of US-American constraint": in its reluctance to expand its wars further in the Middle East, the US weakened the popular legitimacy of the liberal order. Trump, in swerving to the opposite pole of diplomatic sabotage, also failed to strike the right balance in the use of US power. Where Obama had damaged the liberal order through restraint, Trump had trampled it through alienating European allies, opening the field to rising Russian and Chinese challengers. Kagan's counsel is that military assertion must always remain in reserve, but it is to be deployed strategically: allies are not to be ruthlessly treated in all respects, especially economically, and must be accommodated so that all "seek mutual advantage in the interests of free trade."[24]

The timing of Kagan's prospectus coincided with the quadrennial US National Defense Strategy, which marked a decisive shift. In the 2018 NDS, the Pentagon for the first time identified Russia and China as "revisionist powers" whose threat to US and

17 Zbigniew Brzezinski, *The Grand Chessboard* (New York: Basic Books, 1997), 30.
18 Ibid., 41.
19 Zbigniew Brzezinski, *Strategic Vision* (New York: Basic Books, 2012), pp. 125-6.
20 Ibid., 102.
21 Robert Kagan, *The Jungle Grows Back: America and Our Imperiled World* (New York: Knopf, 2018), 108, 112.
22 Ibid., 117.
23 Cf. "Europe's populists are waltzing into the mainstream," *The Economist*, 3 February, 2018.
24 Kagan, *The Jungle Grows Back*, 137.

international interests required greater investment in nuclear forces, space and cyberspace warfare and surveillance. The NDS also called for a fortification of the NATO alliance, by which it meant an expected increase in European military and weapons budgets.[25] The US, under Obama, had already initiated a trillion-dollar nuclear expansion, and by 2020 it had withdrawn from the Intermediate-Range Nuclear Forces treaty, restarted testing of medium-range missiles and terminated the Open Skies Treaty which had allowed for mutual Russian-US monitoring of military preparations.[26] The Joint Artificial Intelligence Center, also launched in 2018, was designed to integrate the Pentagon's use of AI capabilities into civil society, and to accelerate the funding for private companies through the Defense Advanced Research Projects Agency (DARPA). In the Pentagon's own summary report, the Center is described as a response to Chinese and Russian programs, and one that will rely on "allied, coalition partners" as a strategic consideration.[27]

Such efforts have found willing counterparts within the EU establishment, notwithstanding the occasional diplomatic throat-clearing over the course of the Trump term. In 2019, Claudia Major of the German Institute for International and Security Affairs (SWP), identified a "revisionist and aggressive foreign policy of Russia" as a spur to strengthen the NATO alliance, which EU powers should welcome as US-led; European security was for good reason dependent on US nuclear and conventional capacity, especially in defending it against Russia's eastern and southern encroachments since 2014.[28] China, which Major identified as principally an economic and trade contender, nevertheless required NATO's attention given its commercial dealings in Africa, the Near East and its investment in Europe's critical infrastructure, ports above all, as illustrated by the PRC's Italian link in its Belt-and-Road Initiative.[29] The point has recently been reiterated in co-authored paper for the German Council on Foreign Relations (DGAP), in which the US's former ambassador to the EU, Victoria Nuland, has argued that Moscow's "new weapons and hybrid warfare" as well as its "disinformation" efforts, combined with China's "heavy investment in European strategic infrastructure," and "rising military capability," require a renewed and consolidated NATO-EU strategy. Nuland et al. suggest that NATO's eastern base rotations should become permanent, and that greater military spending by EU states, as well as an export regime for "dual use" technologies must be on the agenda.[30]

25 *Summary of the 2018 National Defense Strategy of the United States*, pp. 6, 9. Surveillance here is defined as "command, control, communications, computers and intelligence, surveillance, and reconnaissance," or C4ISR. By December 2019 a new branch of the US armed forces, Space Force, was authorized by Congress in an overwhelmingly bipartisan vote.
(https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf)

26 "In modernizing nuclear arsenal, U.S. stokes new arms race," *Reuters*, 21 November, 2017.

27 According to the AIS, "[o]ther nations, particularly China and Russia, are making significant investments in AI for military purposes...These investments threaten to erode our technological and operational advantages and destabilize the free and open international order. The United States, together with its allies and partners, must adopt AI to maintain its strategic position..." See *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, pp. 5-6.
(https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF)

28 Claudia Major, *Die Rolle der Nato für Europas Verteidigung (Berlin: SWP-Studie, 2019), pp. 6, 12.*

29 Ibid., 14.

30 Christian Mölling, Sophia Becker, Victoria Nuland, "Security and Defense: Transatlantic Action Plan" *DGAP Online Commentary*, 15 February 2021, pp. 2-3, 6. In 2014 Nuland was embarrassed by a leaked phone call to US ambassador to Ukraine, in which she railed against EU's failure to confront Russia in Ukraine and advocated bypassing it by recourse to a UN imprimatur. See "Leaked audio reveals embarrassing U.S. exchange on Ukraine, EU," *Reuters*, 7 February, 2014. Nuland is the spouse of Robert Kagan.

NATO AND THE EXPANDED CONCEPT OF SECURITY

In addition to new geopolitical orientation toward Russia and China, an expanded concept of security has been central to NATO's new strategic footing. As part of the NATO 2030 agenda, the organization has prioritized so-called hybrid warfare – incorporating disinformation, propaganda and artificial intelligence programs – which exists by definition as much in civil society as in strictly military domains.[31] NATO strategists identified such hybrid methods as undermining NATO's "shared democratic identity," under particular strain since the world economic crisis of 2008, and determined that the contemporary impasse "more closely resembles the pre-1989 period when [NATO] was a bulwark of democracy against an authoritarian challenger."[32]

In point of fact this process of expanding definitions of NATO's security portfolio, both geographically and differentially within society, exists in historical continuity with its post-1989 existence.[33] By the early 1990s, as Birgit Mahnkopf identified in 2004, NATO increasingly took on new global missions pertaining to the management of civil society.[34] No longer defined principally by East-West conflict between states, the expanded concept of security anticipated a form of perpetual civil war, or "low-intensity conflict" in which domestic security would be paramount.[35] NATO's contemporary departure should thus be understood as a consolidation of both interstate strategy vis-à-vis state rivals, *simultaneously* and *alongside* a renewed effort to advance its own hybrid warfare programs.

The Western hybrid tactics now called for by the NATO 2030 agenda were anticipated more than twenty years ago by military historian Martin van Creveld, as well as Qiao Liang and Wang Xiangsui within the Chinese military establishment. For the latter, the new concept of warfare would "transcend the domain of traditional weapons," would be "controlled and manipulated at a technical level"; and it would inflict "material or psychological casualties on an enemy" by means of "commonplace things."[36] The People's Liberation Army (PLA) traced this dynamic to the US military's bureaucratic interest in sustaining a threat sufficiently large enough to justify preparations for victory in a major war.[37] Van Creveld, for his part, noted that "the day-to-day burden of defending society against the threat of low-intensity conflict will be transferred to the booming security business."[38] By the end of the 1990s, with its air campaign against Yugoslavia, NATO initiated its first-ever offensive operation waged under an expanded concept of humanitarian war. This followed its eastward expansion into former Warsaw Pact countries, in violation of the agreement struck between Mikhail Gorbachev and George H.W. Bush.[39] NATO's 1999 bombing of Yugoslavia coincided with that year's increased US military expenditure, the first after a several years of stasis.[40] The twenty-year period since has been characterized by the use of private security contractors – from on-the-ground mercenaries, to digital surveillance, to the use of cyberweapons like the US-Israeli Stuxnet – against a backdrop of perpetual NATO war.[41]

31 In a November 2020 report, a NATO advisory group identified "emerging and disruptive technologies" and "military-civil fusion" in China as a reason to develop a "North Atlantic equivalent of the US Defence Advanced Research Projects Agency (DARPA) or European Defence Fund (EDF)." *NATO 2030: United for a New Era*, pp. 30-31.
32 "NATO's political role more closely resembles the pre-1989 period when it was a bulwark of democracy against an authoritarian challenger." Ibid., p. 20.
33 Chalmers Johnson had already by 2000 documented the growth of a stealth US empire, and the hatred it provoked across, *inter alia*, northern Italy and Okinawa, sites of large US military bases. See Chalmers Johnson, *Blowback: Costs and Consequences of American Empire* (New York: Henry Holt, 2000).
34 See Birgit Mahnkopf, "Neoliberale Globalisierung und Krieg", in: Blätter,1/2004, pp. 47-57, 50. This was a view advocated at the time by US State Department deputy Richard Holbrooke. See Holbrooke, "America, a European Power," *Foreign Affairs* Vol. 74 No. 2 (1995), pp. 45-6.
35 See also Lange, "Sicherheitsbegriff, erweiterter," in Hans-Jürgen Lange (ed.), *Wörterbuch zur Inneren Sicherheit (Wiesbaden: Springer, 2006), p. 288.*
36 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing, 1999), pp. 25-6.
37 Ibid., 127.
38 Martin van Creveld, *The Transformation of War* (New York: Simon & Schuster, 1991), 207.
39 Svetlana Savranskaya and Tom Blanton, "NATO Expansion: What Gorbachev Heard," National Security Archive Briefing Book 613 (https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early).
40 Philip Cunliffe has identified 1999 as the opening year of a period extending to 2019. See Cunliffe, *The New Twenty Years' Crisis: 1999-2019* (Montreal: McGill-Queen's University Press, 2020), pp. 44-8.
41 Stuxnet was a piece of digital software used to inflict material damage on Iranian infrastructure. See "Stuxnet Was Work of US and Israeli Experts, Officials Say," *Washington Post.* 2 June, 2012.

ESCALATION AT THE TURN OF THE CENTURY

Renewed US militarization dating from 1999 and NATO's new eastward-oriented offensive war footing went into overdrive by the fall of 2001, with the US-NATO invasion of Afghanistan in the aftermath of the September 11th attacks. The information warfare component of the new "war on terror," including surveillance and secrecy, expanded the extant security apparatus's reach into civil society.[42] The proposed Total Information Awareness Agency called for a global infrastructure of continuous and warrantless mass surveillance, later realized as the NSA's PRISM and related programs, including those of deception, dissimulation and misdirection, as revealed by Edward Snowden.[43] The period also saw the global debut of CIA-run black sites for kidnapping, indefinite detention without charge and torture.

Expanded surveillance and covert operations under the global war on terror entailed disinformation. Contemporary with the NATO war on Afghanistan was a highly orchestrated disinformation campaign to convince the public of Saddam Hussein's obstinate refusal to disarm his weapons of mass destruction, including biological weapons then associated in the public mind with the anthrax mailings in the United States of October 2001. In reality, from the conclusion of the Gulf War in 1991, the US-UN sanctions against Iraq, combined with its inspection regime and no-fly zones, had reduced the country to a state of abject poverty in which it is estimated that hundreds of thousands of children died for lack of medical equipment and essential medicines.[44] Iraq posed no threat to the United States and Europe. The effort by the US authorities to persuade EU and NATO member states to join in the attack on it will constitute for this report one historical case study in which the destruction of the Near East, undertaken on the basis of fabrication and falsehood, illustrates the US's recent and unambiguous use of disinformation in the course of achieving its war aims.

42 For discussion of some of the cultural consequences of the security programs, as well as their historical origins, see Joseph Masco, *Theater of Operations* (Durham: Duke University Press, 2014), *passim* and p. 131.

43 "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian*, 7 June, 2013. The British equivalent of the NSA, GCHQ, was revealed by Snowden to have trained its agents to deceive the public in "online covert operations." See the document "The Art of Deception," published by *The Intercept*: https://theintercept.com/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/

44 Patrick Cockburn, *The Age of Jihad* (London and New York: Verso, 2017), pp. 38-46.

THE WAR ON IRAQ: A STUDY IN US DISINFORMATION

Nearly two decades on, the concatenation set off by the US-UK attack on Iraq in March 2003 shapes the geopolitics of the Levant, the Maghreb and beyond. In Europe, the political consequences are most clearly felt in the influx of refugees fleeing its aftershocks. Yet the Iraq war has also altered the internal politics of the West profoundly, in its effect on civil society. An accelerant to the US's global war on terror, the war remains an index of the overt brutality of its security services and their capacity for fabrication, deception and bellicosity, aimed especially at a domestic or allied, rather than an ostensible "enemy" public. In the US and UK, the major architects of the war have never been brought to book, and much of the specific nature of the disinformation efforts in its lead-up remains murky. The campaign of fearmongering necessary for creating the appearance of a just cause for war enjoyed open, material support of prime ministers José María Aznar of Spain and Tony Blair in the UK, and the tacit support of others, like Silvio Berlusconi of Italy.

For Europe, which was formally a minor player, the Iraq war posed a unique set of problems. The war split the West from the beginning, and the US propaganda effort did little to convince the European public that it was necessary to back it. Aside from the UK leadership, which made much of its "special relationship" with its American ally, only Spain and Poland formally joined the war effort from the start, although NATO did deploy an advisory mission in 2004, which it has recently renewed. Nevertheless, European governments were party in certain important respects to the drive to war, even if this activity was clandestine, or later disputed or disavowed.

With respect to disinformation and foreign interference, four components in the Iraq War case stand out. The first was the process of manipulation of human intelligence gathered by US security services at the behest of White House officials and principally British accomplices. This involved European, including especially German and Italian intelligence agencies, whose operations were closely tied to those of the Americans and therefore implicated in the political case made by the Bush White House. Second was the surreptitious use of compliant elements within mainly the US press, above all at the agenda-setting *New York Times*, to launder falsehoods about the Iraqi threat, and to give them the imprimatur of an independent and even adversarial organ normally associated with the opposition – that is, Democratic – party.[45] Third: the Iraq War security footing invited a massive expansion of the global war on terror, and implicated, as has been mentioned, European jurisdictions in the war effort at both covert and public operational registers. This included the complicity of Italian intelligence services in laundering US claims of Iraqi weapons programs, an instance in which a European power covertly subverted the will of its public constituency. Fourth: the aftermath of the war redounds to this day in the form of a successive of regional crises and wars – in Syria, and by proxy in heightened US bellicosity toward Iran – all of which burden the politics of immigration to Europe, the EU's geostrategic orientation toward Russia and the "pivot to Asia" as reflected in the NATO 2030 communiqués.

MANIPULATION OF INTELLIGENCE

Mobilization for a full-scale US war on Iraq began immediately after the September 11th, 2001 attacks. The war was premised first on alleged linkages between the Iraqi state and Al Qaeda, and secondly on allegations of Iraq's continuing biological, chemical and nuclear weapons programs – both false. Each reason in turn was supported by the US security apparatus: the former, by National Security Council over the course of 2001-2003, and principally by the close circle of neo-conservative advisers around then vice president Dick Cheney: Paul Wolfowitz, Lawrence Libby, Richard Perle, and the secretary of defense Donald Rumsfeld, all of whom were drawn from the Project for a New American Century think tank or the affiliated American Enterprise Institute.[46] The WMD case was pushed more broadly and was central to UK support. The exact role of the main US's main intelligence service, the CIA, especially with respect to the neo-conservative group around Cheney, became a matter of internal dispute once the Iraqi resistance to US occupation scotched the swift victory that had been promised to the American public.

45 The 2002 vote to authorize the attack on Iraq was fully bipartisan, and was supported by prominent Democratic politicians, including Joe Biden, Hillary Clinton and John Kerry.

46 PNAC was founded in 1997 by neo-conservatives William Kristol (its chair) and Robert Kagan. In an open letter to Bill Clinton in 1998, it enlisted two dozen signatories, many of whom would later join George W. Bush's White House staff or cabinet, to demand a strategy of increased militarism designed to forestall any challenges to US geopolitical supremacy. PNAC recommendations included stepped-up belligerence against Iraq. Clinton, for his part, in addition to routine enforcement of the so-called "no-fly zones" in Iraq and the murderous UN sanctions, ordered a four-day bombing campaign of the country in December 1998.

As a result, then-director George Tenet, in his 2007 memoir, shifted the blame for the drive to war squarely onto Cheney's office. Tenet claimed that he was unaware of the seriousness of the White House's commitment to war until it was too late.[47]
Yet as early as the spring of 2002, even the British had committed themselves to the attack on Iraq, which hardly could have escaped the CIA's attention. Decisively, the National Intelligence Estimate (NIE) of October 2002, the statement published on behalf of all eighteen US intelligence agencies, warned that "Iraq has continued its weapons of mass destruction (WMD) programs..." and cited specifically the production of poison gases, such as mustard and sarin and VX nerve agents, as well as "large-scale, redundant, and concealed BW [biological weapons] agent production capability" that was then "offensive" and "larger and more advanced than...before the Gulf war." According to the 2002 NIE, Baghdad sought "aluminum tubes for centrifuge rotors," which it asserted was evidence that "Saddam is reconstituting a uranium enrichment effort for Baghdad's nuclear weapons program."[48] Blair's meeting with Bush in April of 2002 was responsible for a strategy of pursuing UN Resolution 1441, which put Iraq in a position of having to prove it was complying with the disarmament of weapons it did not have. This was the British-American cover for the attack, as revealed in 2005 through a leak of the so-called "Downing Street Memo" of July 2002, in which the head of MI6, Richard Dearlove had reported that "[m]ilitary action was now seen as inevitable."[49]

This strategy was followed dutifully by multiple European governments, as expressed by the January 2003 "Letter of Eight," signed – aside from Blair himself – by the heads of government from the Czech Republic, Denmark, Hungary, Italy, Spain, Poland and Portugal.[50] The letter took as a given Iraq's "denial and non-compliance" with UN Resolution 1441, and its possession of "weapons of mass destruction," whose "combination" with "terrorism" posed "a threat of incalculable consequences."[51] Italy specifically was essential to this disinformation campaign. Indeed, it was an Italian intelligence agent, Rocco Martino, who furnished the British with the fabricated report that Iraq had sought yellowcake uranium from Niger, part of Berlusconi's bid to ingratiate himself with the Anglo-American axis.[52]

This special role played by Italian intelligence in the Iraq war merits additional discussion. Two reporters for *La Repubblica*, Carlo Bonini and Giuseppe D'Avanzo, in 2007 published their discovery of extensive collaboration between Dick Cheney's office and the Italian foreign intelligence agency, SISMI. Central to the Bonini and D'Avanzo's account is the repeated use of "competitive intelligence," or the laundering of information – by reconfirming planted stories – across various services and media.[53] Nicolò Pollari, SISMI's head at the time of the US drive to war in 2002-03, revived in serial fashion, the demonstrably bogus claims dating from the late 1990s, made by a former agent Martino regarding Nigerien uranium, as well as fraudulent claims of Iraqi purchases of aluminum tubes for enriching the element. Although Martino's fabrications of uranium export to Iraq were likely originally motivated by the prospect of selling supposed valuable intelligence – in the form reality fabricated documents – to French counterparts, the matter took on special geopolitical significance in the context of the lead-up to the US war years later. It was then that SISMI, in collaboration with Pentagon's Office of Special Plans, run directly by Cheney's deputy Douglas Feith, revived Martino's counterfeit evidence, removed the most egregious signs of forgery and set them in motion to be used as *casus belli*.[54]

The key source of US allegations of biological weapons was intelligence also brought in from European services. Germany's agents supplied information to the US Defense Intelligence Agency statements of an Iraqi defector, code-named Curveball, who was made available to the US by the German Federal Intelligence Service (BND). In 2011, the BND chief at the time, August Hanning, condemned US fabrications, and asserted that "the U.S. misused the BND for its justification of the Iraq war."[55] According to Hanning, Curveball, who had defected in 1998, was unreliable, and though the BND had initially refused the Americans access to him, it relented in the period leading up to Colin Powell's 2003 speech to the UN Security Council,

47 In his 2008 memoir, Tenet argued that the CIA was under pressure to manufacture the false connection, principally by way of backing faulty evidence of an alleged Prague meeting between September 11th hijacker Mohamed Atta and an Iraqi agent. Tenet maintained that he had felt there was insufficient evidence on this point, though the White House's NSC backed it. For a review of Tenet's memoir and its weaknesses, see Thomas Powers, *The Military Error* (New York: NYRB Collection, 2008), pp. 106-08.
48 See "National Intelligence Estimate 2002-16HC," October 2002, pp. 5-7. The declassified document, and discussion of it, is available at the National Security Archive website: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB129/
49 Mark Danner, "The Secret Way to War," *New York Review of Books*, 9 June 2005.
50 Respectively, Václav Havel, Anders Fogh Rasmussen, Péter Medgyessy, Silvio Berlusconi, José María Aznar, Leszek Miller, José Manuel Barroso. The full text of the letter, "Europe and America Must Stand United," can be seen at: https://archive.globalpolicy.org/security/issues/iraq/media/2003/0130useur.htm
51 Ibid. The signatories also reaffirmed "the transatlantic bond."
52 See Powers, *The Military Error*, p. 118-19.
53 Bonini and D'Avanzo quote a former CIA field officer who defines the term as follows: "A piece of intelligence, normally provided by a source who tells you exactly what you want to hear, is passed along to an allied intelligence agency or to another source, who will pass the 'news' in turn to a friendly agency...While our intelligence agencies are searching for proof, allied agencies keep popping up with the same news...the news is repeatedly confirmed." See Carlo Bonini and Giuseppe D'Avanzo, *Collusion: International Espionage and the War on Terror* (Hoboken: Melville House, 2007), 43.
54 Ibid., pp. 44-8, 58.
55 See "USA haben BND für Irak-Krieg missbraucht," *Die Welt 27 August, 2011.*

even though the information on which it was based – Curveball's testimony – was unverified and doubted.[56]

For its part, the US, facing steep odds on a second UN resolution authorizing use of force, mobilized the NSA to direct its British counterpart, the surveillance service GCHQ, to gather information on holdouts so as to pressure them to support it. A memo containing instructions to this end, leaked by GCHQ agent Katherine Gunn to *The Observer*, revealed that the US agency expected the GCHQ to focus surveillance on UN Security Council members in the period after the weapons inspection team led by Hans Blix had reported Iraqi compliance with the Resolution 1441.[57]

USE OF MEDIA

Gunn's leaked NSA/GCHQ memo was a rare instance of pre-war critical coverage by the Anglo-American press. Its publication by *The Observer*, on 2 March 2003, took place shortly before the US-UK bombardment, which began on 19 March. More characteristic of press treatment of the war was the mobilization across the political spectrum to promote the same false story favored by the White House and 10 Downing Street, with varying degrees of emphasis put on one or another of the two poles of the official US-UK framework. In this telling, Saddam Hussein was either guilty of a "failure to disarm," and therefore was inviting the looming attack himself, which, however regrettable, would be necessary to enforce the will of the so-called "international community"; or, secondly, Saddam Hussein posed such an imminent threat, and had demonstrated a willingness and capacity to use unconventional delivery of his WMD, that unilateral and pre-emptive war was already justified. Generally, the emphasis on the first point, mixed with some humanitarian rhetoric, was taken as the liberal or centrist rationale. The second was openly the preference of the Bush White House, and indeed was the one that ended up serving as the *de facto* justification once NSA pressure and Powell's fabricated presentation to the UN about WMD had failed to mobilize enough of the General Assembly in winning a second resolution authorizing war. Most statements mixed aspects of the two, and varied by degree rather than categorically. Yet in the pages of the major newspapers, throughout the period of 2001-2003, the central falsehood that Iraq possessed WMD was not questioned.[58]

US claims that Iraq possessed WMD, specifically that it was capable of producing anthrax and that it was seeking nuclear weapons-grade uranium, were themselves not only immune to critical scrutiny, but in some instances were planted in newspapers such as the *New York Times* by reporters working with US government officials, whose identities they concealed. In this aspect, the Anglophone press served as a major source of disinformation about WMD, and this basic falsehood was the framework under which nearly all debate – narrowly construed, with the major question of war or peace already decided – took place.[59] Among the most potent disinformation campaigns was the reporting by Judith Miller of the *New York Times*. From 2001 to 2003, Miller's output made use of two Iraqi sources, in addition to anonymous and unverified government sources: Ahmad Chalabi, a patrician exile associate of Curveball promoted by the American Enterprise Institute and in the pay of the CIA, US State Department and Pentagon from the 1990s, and the defector Khidir Hamza, whose credibility was doubted by the International Atomic Energy Agency (IAEA). This reporting, which advanced claims that Hussein was on a quest for atomic bomb technology, and was in possession of biological weapons and posed an imminent threat, was then cited by White House officials in highly coordinated television appearances.[60] In 2005 Miller was revealed to have been in close contact with the vice president's adviser I. Lewis Libby, in the course of the latter's effort to retaliate against a dissident report which undermined the false US claims of Iraqi uranium purchases.[61]

56 Powers, *The Military Error*, 116.
57 See "US plan to bug Security Council: the text" in *The Observer*, 2 March 2003, and "Revealed: US dirty tricks to win vote on Iraq war," 2 March 2003.
58 See, for instance, *The New York Times* editorial of 15 February, 2003, "Disarming Iraq," in which the editorial board opined that "[t]here is ample evidence that Iraq has produced highly toxic VX nerve gas and anthrax and has the capacity to produce a lot more," and that, because Iraq was not disarming, the Security Council must prepare "to call in the cavalry to get the job done" – a decision that America and Britain had already, rightly, decided on in the affirmative. (https://www.nytimes.com/2003/02/15/opinion/disarming-iraq.html).
59 Statistical analysis by Danny Hayes and Matt Guardino has documented an "absence of domestic elite dissent," cast in the broadest possible terms, i.e. as support for a resolution by "diplomatic" means: either a return to the *status quo ante* of UN sanctions, or a second UN resolution to authorize force. Nevertheless, the Bush administration, even by this generous standard of what qualified as "dissent," enjoyed overwhelming support from the print and broadcast media across the board. See Danny Hayes and Matt Guardino (2010) "Whose Views Made the News? Media Coverage and the March to War in Iraq," *Political Communication* 27: 1 (2010), pp. 75-6, 81.
60 See Michael Massing, "Now They Tell Us," *The New York Review of Books*, 26 February, 2004 and Bonini and D'Avanzo, *Collusion*, pp. 78-82.
61 "Cheney's aide revealed as source of CIA leak," *The Guardian* 1 October, 2005.

In contrast to Miller's steady drumbeat of pro-war reporting, which appeared on the front page of the *Times*, the IAEA inspectors' determination in January 2003 that Iraq had made no meaningful progress toward acquiring an atomic weapon was buried inside the paper. Colin Powell's UN presentation, which contradicted the findings of the weapons inspectors, however, enjoyed favorable – and also featured – coverage in the *Times*, as it did in the *Washington Post*. Although the *Post* had covered IAEA director Mohamed El-Baradei's dissident conclusions, in an editorial on 6 February, 2003 it deemed Powell's UN speech "irrefutable": "After Secretary of State Colin L. Powell's presentation to the United Nations Security Council yesterday," the *Post* lectured, "it is hard to imagine how anyone could doubt that Iraq possesses weapons of mass destruction."[62] Yet at the time, Scott Ritter, a UN weapons inspector in Iraq from 1991 to 1998, was attempting to deflate the allegations of Iraqi WMD. Ritter based himself on extensive direct experience and knowledge, which had led him to conclude, already in 2000, that

> Given the comprehensive nature of the monitoring regime put in place by UNSCOM, which included a strict export-import control regime, it was possible as early as 1997 to determine that, from a qualitative standpoint, Iraq had been disarmed. Iraq no longer possessed any meaningful quantities of chemical or biological agent, if it possessed any at all, and the industrial means to produce these agents had either been eliminated or were subject to stringent monitoring. The same was true of Iraq's nuclear and ballistic missile capabilities.[63]

Ritter furthermore argued Iraq could not have been able to restart programs disarmed since 1998, and that the main obstacle to reintroduction of inspections was the stated US policy of regime change. Ritter's warnings in 2002 were picked up by CNN, but the *New York Times* and *Washington Post* both attacked him. A report for the *Times* titled "Scott Ritter's Iraq Complex," for example, was comprised of little more than *ad hominem*, in which its authors surmised features of Ritter's psychology and asserted these qualities as the source of his conclusions and reasoning regarding the status Iraqi weapons.[64]

The overall effect of the coverage by the *Times* and *Post* was a deemphasis on current and past inspectors' conclusions by ignoring, burying or undermining them through attacks on character; when combined with the promotion of dubious and even outright false allegations provided by sources linked to pro-war organizations inside and closely aligned with the US and UK, these reports shaped US and to an extent global public opinion in such a manner that Iraq was understood to be an imminent threat, due to its WMD capacity and links to organized terrorism.[65]

CONSEQUENCES

The immediate and long-term consequences of the successful drive to war for the peoples of the Middle East and North Africa cannot be rehearsed in great detail here. They are apparent in the arc of destruction unleashed by the American offensive. For Europe, blowback from Spanish and British participation in the invasion was swift, in the form of bombings in Madrid and London of 2004 and 2005. In the period between then and the spring of 2014, the theater widened significantly to encompass a mutating Iraqi civil war which had been ignited in 2006 among opposing US-backed belligerents. Once the 2011 NATO attack on Libya saturated the country with arms, the US moved quickly to back rebel groups in Syria, where by 2013 it had opened up a new front of air and ground operations. The Islamic State, itself a product the Iraq invasion and ensuing civil war, rapidly consolidated territorial control from Mosul and Fallujah in Iraq to eastern Syria, and by the summer of 2015 the crisis had detonated the largest global migration since the Second World War.[66] A second wave of attacks in Paris and Berlin, followed by recent events in Vienna, has yielded periodic states of emergency and a general coarsening of European public life.

62 See "Irrefutable," *The Washington Post*, 6 February, 2003. For further discussion, see Massing, "Now They Tell Us," *The New York Review of Books*, 26 February, 2004.

63 Scott Ritter, "The Case for Iraq's Qualitative Disarmament," *Arms Control Today*, June 2000. (https://www.armscontrol.org/act/2000-06/features/case-iraqs-qualitative-disarmament). UNSCOM – the United Nations Special Commission – was the UN inspection body in existence between 1991 and 1999 overseeing Iraqi disarmament. For Ritter's judgment in 2002, see "Scott Ritter: Facts Needed Before Iraq Attack," *CNN*, 17 July, 2002.

64 A representative passage: "Even when admitting he is wrong, he is insisting he is right. His self-image requires it, for more than a life story, he has a personal mythology." See "Scott Ritter's Iraq Complex," *The New York Times*, 24 November, 2002. For further discussion of the media treatment of Ritter, see Seth Ackerman, "Right Too Soon?" *FAIR*, 1 September 2003 (https://fair.org/extra/right-too-soon/).

65 Amy Gershkoff and Shana Kushner, "Shaping Public Opinion: The 9/11-Iraq Connection in the Bush Administration's Rhetoric," *Perspectives on Politics* Vol. 3 No. 3, Sep 2005: p. 531.

66 "Worldwide displacement hits all-time high as war and persecution increase," Statement of the United Nations Refugee Agency, 18 June, 2015: https://www.unhcr.org/news/latest/2015/6/558193896/worldwide-displacement-hits-all-time-high-war-persecution-increase.html

In the US, from the midterm elections of 2006 through the Barack Obama presidency, the two parties committed themselves to escalation, even as popular disgust with official disinformation and destruction mounted. Having run on an "anti-war" platform, the Democrats retook the House and Senate at the end of 2006. But, by rejecting any investigation into the lead-up to the war and in funding it without question, they indicated a feature of the party's activity that would grow clearer once Obama entered the White House in 2009. Drone war, surveillance and cover-up of Bush crimes – a classified copy of the US Senate's investigation into CIA torture was deleted from the agency's servers, as it infiltrated Senate computers[67] – effectively consolidated the two parties now formally into one pro-war bloc, where the arrangement had previously appeared more ambiguous. From the middle of Obama's second term, prominent neo-conservatives, including Robert Kagan and William Kristol, moved to back Democrats, which they have now done consistently since 2016.[68]

In the period since this political consolidation, many of the powerful intelligence officials involved in the lead-up to the Iraq invasion have found lucrative work in US media, where they continue to warn of foreign threats. James Clapper, previously of the National Geospatial-Intelligence Agency, furnished the images of alleged weapons of mass destruction – the basis for an expedited schedule for war – before taking the cabinet-level position of director of national intelligence in 2010. From this position, he oversaw a global, illegal spying operation on digital communications, and was not above lying to the US Congress about the program. Since 2017, Clapper has been a "national security analyst" for CNN along with his one-time deputy, former NSA and CIA director Michael Hayden, who oversaw and defended publicly the CIA's secret torture program once it was revealed. Though he has since retired from public life, Hayden continues to work at the Chertoff Group and the Atlantic Council.[69]

John Brennan, the director of national counterterrorism under George W. Bush, also defended the torture program until 2009, when he was incorporated into the Obama administration, first as a trusted national security adviser, and then CIA director in his own right. He is now a paid consultant for the US cable network MSNBC, which is marketed to US Democratic Party voters, and through which he has issued a flood of warnings about foreign interference based on little other than the say-so of colleagues with the US security services.[70] In the period since the electioneering of 2006, a revitalized and rehabilitated official deceit has endured.

67 See "CIA Hacked Senate Computers," *Newsweek*, 31 July 2014 and "CIA says mistakenly 'shredded Senate torture report then did not," *Reuters* 17 October 2017.

68 See "The Next Act of the Neocons," *The New York Times*, 5 July 2014, "Prominent GOP Neoconservative to Fundraise for Hillary Clinton," *Foreign Policy* 23 June, 2016. In 2019 Biden's secretary of state Antony Blinken co-authored an opinion piece with Kagan.

69 The Chertoff Group, a security consultancy and lobby, was founded in 2009 by Bush's former secretary of homeland security, Michael Chertoff. Chertoff also sits on the boards of the Atlantic Council and NATO's Slovakian think tank GLOBSEC. See pages 33 and 34 of this report for further discussion.

70 Bush himself recently took to US television to express his alarm at "how much misinformation there is and the capacity of people to spread all kinds of untruth." See "Bush: Today's GOP is 'isolationist and 'nativist'" *Politico* 20 April 2021. For a compilation of the most outlandish claims of this type, see Glenn Greenwald, "How Do Big Media Outlets So Often 'Independently Confirm' Each Other's Falsehoods?" *Substack* 16. March 2021.

02

NATO'S THINK TANKS IN CENTRAL AND EASTERN EUROPE

As with the US-led Iraq war and global war on terror, management of European public opinion is central to US reorientation toward "revisionist powers" outlined in its 2018 National Defense Strategy.[71] A network of NATO-linked think tanks in eastern and central Europe, including the Centers of Excellence and, separately, the Slovakian GLOBSEC, are one component of this effort. These organizations deal in digital and cyber warfare, public relations and the consolidation of civil society behind NATO's priorities on its eastern flank. Through their activities they aim to shape public opinion directly through so-called strategic communications and the publicity generated by conspicuous military drills and conferences.

Exemplary of NATO's use of these think tanks for its information warfare efforts is the cluster NATO's Baltic centers. They often work closely with Washington's Atlantic Council, but mobilize local military strategists and politicians, and appeal to wider European audiences.[72] In July 2018, the chair of the Latvian parliament's (or Saeima's) foreign affairs committee, Rihards Kols, warned of ongoing Russian hybrid warfare against NATO. Kols's statement, which appeared in a blog hosted by the Atlantic Council (where he is also a "millennium fellow") presented a frightful image of Russia's "use of military force and hybrid tactics" now calling into question "NATO's ability to defend its eastern borders." Among the weapons employed by the Kremlin to destabilize the West, Kols claimed, were information operations, cyberattacks, disinformation and other propaganda and psychological operations – which might also encompass "organized crime, sabotage."[73]

Kols claimed a Russian offensive had infiltrated all media, new and traditional alike, and therefore recommended an escalation of NATO countermeasures, for which the Centers of Excellence, especially those established in the Baltic, should be expanded.[74] Dissatisfied with their exclusive focus on analysis and research, however, he advised that they "operationalize" their capabilities, and "develop practical and concrete recommendations, action plans, and clearly articulated strategies." Kols furthermore urged NATO member states to "share knowledge and prove better dissemination of intelligence across the Alliance," and predicted that "vulnerability and chaos are not only the product of destabilization efforts, but also the prelude to overt conflict."[75]

The Atlantic Council's belligerent summary of Baltic politics reveals much about what NATO has organized for the region. Although its Centers of Excellence are not formally integrated into the alliance's command structure, they are subvented by its member states, which join them on an *ad hoc* basis. They draw on NATO personnel for their research and activities, which include academic-style reports as well as war games. The centers appear to run a light-touch program, with annual budgets kept in the mid-six-figure range.[76] Yet, as the following profiles indicate, they and the similarly organized GLOBSEC more than compensate for their modest staffing and expenditure in their ability to generate sympathetic coverage for the sort of rhetoric deployed by Kols.

71 For insight into the US public relations strategy in Europe with respect to its war in Afghanistan, see the leaked March 2010 CIA memo "Afghanistan: Sustaining West European Support for the NATO-led Mission–Why Counting on Apathy May Not Be Enough," *Wikileaks* release 26 March 2010.

72 Founded in 1961, the Atlantic Council was previously an adjunct to NATO. It has since broadened its range. See Justine Drennan, "Call of Duty: Star Video Game Director Takes Unusual Think Tank Job," *Foreign Policy, 22 September, 2014*.

73 Kols is also Latvia's delegate to the OECD. See Rihards Kols, "NATO Must Meet Russia's Hybrid Warfare Challenge," *New Atlanticist*, 3 July, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-meet-russia-s-hybrid-warfare-challenge/. For an overview of the Atlantic Council in relation to other security and defense-oriented think tanks, see James G. McGann, "2020 Global Go To Think Tank Index Report," *TTCSP Global Go To Think Tank Index Reports*. 18., p. 136.

74 The Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallin, and the Strategic Communications Centre of Excellence (StratCom COE) in Riga represent a significant "move toward addressing hybrid threats."

75 Kols, "NATO Must Meet Russia's Hybrid Warfare Challenge."

76 Germany sponsors fifteen NATO CoE, to which it supplies 102 staff and contributes €996,702 annually. See the Answer by Federal Government to Die Linke's parliamentary inquiry, August 10, 2021, Bundesdrucksache 19/31789, p. 3 (https://dserver.bundestag.de/btd/19/319/1931975.pdf).

THE COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE)

The Cooperative Cyber Defence Centre of Excellence (CCDCOE) is an Estonian-based think tank founded in Tallinn in 2008 under the supervision of the governments of Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain.[77] Now funded and staffed by an expanded roster of countries, including the United States, Canada and the Republic of Korea, it is among the oldest within the network of NATO-accredited think tanks presently comprised of twenty-six "centers of excellence."[78] As early as 2004, shortly after joining the North Atlantic Treaty Alliance, Estonian representatives had proposed a concept for a cyber defense think tank, and the Supreme Allied Commander Transformation approved the concept in 2006. It took nearly two years before the center was fully operational; alleged cyberattacks against Estonia in the spring of 2007 accelerated its establishment.[79] In its structure of support and funding, the CCDCOE stands out: beyond the twenty-five NATO member states which sponsor it, Austria, Finland, Sweden and Switzerland also finance or staff it – an indication of the broad mobilization of EU and NATO countries in the domain of cyber warfare.[80]

Because NATO-accredited COEs are neither part of the alliance's structures of command, nor funded directly by it, they operate within so-called Framework Nation groups. This *ad hoc* arrangement launches the centers, and may over time take on additional sponsoring countries.[81] No regular overview of the COE budget therefore exists, and exact figures for the CCDCOE's budget in particular remain obscure. When Ireland applied to join it in 2019 – in response to a reported uptick in attacks on the private sector and on its public infrastructure – the country pledged an annual contribution of €22,000 to the costs of running CCDCOE.[82] Germany contributes €82,500 annually.[83] These are the only current indications of the Center's overall budget.

FUNCTION AND PROGRAM

Among the think tank's stated central functions is the coordination of cyber intelligence across its member states. It furthermore focuses on cyber defense research (which also serves a dual use as offensive capability), training, and exercise, undertaken at the request of either the member nations or the NATO command. The Center's areas of focus within the wider field of cyber security are as follows: technology, strategy, operations and law. Within them, the CCDCOE has developed a training portfolio which addresses a wide spectrum of cyber warfare matters, from the technical to the strategic, and concerns itself with its relation to critical infrastructure, law and operations planning. Participants are drawn from the Center's member states as well as permanent NATO staff.[84] Along with its exercises, the Center's conferences attract prominent politicians and technology publicists from the governments, militaries, businesses and academic circles of NATO states and beyond.[85]

Since 2009, the CCDCOE has hosted an annual international conference on so-called "cyber conflict," abbreviated as CyCon.[86] This recurring conference scheme focuses on technical, legal, policy, strategy and military aspects of cyber security. Each year it draws hundreds of military, academic and government participants to Tallinn where attendees present papers, later compiled published, on military strategy and technical aspects of cyber warfare. Keynote speakers have included heads of state, EU officials, NATO's high-ranking military personnel, academics and corporate managers.[87] In 2019 CyCon's sponsors included US software, appliances and services firms

77 See the website of Cooperative Cyber Defence Centre of Excellence (CCDCOE): https://ccdcoe.org/about-us/

78 See the NATO-accredited Centers of Excellence 2021 Catalogue: https://www.act.nato.int/application/files/1916/0686/0400/2021-coe-catalogue.pdf

79 Western media reported at the time that in the aftermath of the Estonian government's 2007 decision to relocate a Soviet statue from Tallinn's downtown area to its suburbs, the country experienced massive cyberattacks on official and commercial websites. The *Guardian*, *New York Times* and *Foreign Policy* attributed the attacks to Moscow, although no definitive link was found, and neither the EU nor NATO accused Russia directly. See for example Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, 17 May, 2007: https://www.theguardian.com/world/2007/may/17/topstories3.russia; Steven Lee Myers, "Cyberattack on Estonia stirs fear of 'virtual war'," *The New York Times*, 18 May, 2007: https://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html; Emily Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?!, *Foreign Policy*, April 27, 2017 https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/; Elizabeth Schulze, "When this country faced a suspected Russian cyberattack – it took some big steps to stop another," CNBC, 21 September, 2018. https://www.cnbc.com/2018/09/21/when-this-country-faced-a-suspected-russian-cyberattack--it-took-some-big-steps-to-stop-another.html.

80 Cooperative Cyber Defense Centre Excellence, "About Us," https://ccdcoe.org/about-us/ and *NATO-accredited Centres of Excellence: 2021 Catalogue*, p. 26. See: https://www.act.nato.int/application/files/1916/0686/0400/2021-coe-catalogue.pdf

81 Ibid.

82 Conor Gallagher, "Ireland to join Nato cyberintelligence sharing agency: Department of Communications denies move is a step towards full NATO membership," 11 October, 2019: https://www.irishtimes.com/news/crime-and-law/ireland-to-join-nato-cyberintelligence-sharing-agency-1.4046808

83 See the Answer by the Federal Government to Die Linke's parliamentary inquiry, 10 August, 2021, Bundesdrucksache 19/31789, p. 2.

84 "Know the CCDCOE: Interview with Director Col. Jaak Tarien," NATO Association of Canada, January 29, 2020, https://natoassociation.ca/know-the-ccdcoe-interview-with-director-col-jaak-tarien/

85 The CCDCOE thus contributes to the formation and reproduction of a "power elite" – drawn from the military, civilian government and industrial sectors – as identified by C. Wright Mills more than 60 years ago, and which now must include academia. See C. Wright Mills, *The Power Elite* (Oxford: Oxford University Press, 1956), pp. 292-94 and *passim*.

86 See the conference's website: https://ccdcoe.org/cycon/

87 For proceedings of the 2019 CyCon, see: https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf.

like Microsoft and Fortinet, as well as the Italian security contractor Leonardo.[88]

THE TALLINN MANUALS: GUIDELINES FOR CYBER WARFARE

In 2009 CCDCOE began drafting the *Tallinn Manual*, NATO'S guideline for cyber war. The project recruited the Center's own staff and legal specialists to a so-called "International Group of Experts," and was produced in consultation with the US Cyber Command, then operating within the National Security Agency. The project, which now includes revised editions, has been directed by Center fellow Michael Schmitt, a former US Air Force judge advocate, specialist in "operational and international law" and professor emeritus at the United States Naval War College, the site of a 1999 conference which the *Tallin Manual* refers to as its earliest predecessor.[89] Schmitt also holds posts at the US Military Academy at West Point and is a member of the Council on Foreign Relations.[90] In 2017, CCDCOE published a second, expanded edition of the manual, welcomed by *Forbes* for alerting governments to looming and pervasive threats.[91] More recently, the CCDCOE has initiated research for a third edition to be completed over the next five years under Schmitt's direction.[92]

The *Tallinn Manual* claims to be the first study devoted to the question of international law's applicability to cyber warfare.[93] Its first edition consisted of ninety-five "rules" to which states would refer in the event of such a war, and addressed the basic questions of the use of force in this new domain. It reiterated states' recourse to claims of self-defense and the specific appeals to the UN Security Council.[94] The manual found that "to date no international armed conflict has been publicly characterized as having been solely precipitated in cyberspace," but nevertheless contended that cyber operations may be considered armed conflict.[95] On the question of attribution and responsibility, the manual determined that states are only to be considered "associated" with operations traced to their infrastructure, and cannot on that basis be held responsible for them; such actions must be committed by an organ of state exercising "governmental authority," which generally excludes those actions undertaken by private groups.[96] The manual also defined the most fundamental terms. It glossed cyberattacks as acts causing "injury or death to persons or damage or destruction to objects,"[97] but notably exempted actions taken against civilians that escaped this narrow definition. "Certain operations directed against the civilian population are lawful," reads rule thirty-one, as in for instance "psychological operations such as…making propaganda broadcasts" or analogous operations "in the context of cyber warfare." Elsewhere, the manual found the use of "ruses" and "false information" to be permissible. Rule thirty-five in any case determined that once they are deemed to have participated in hostilities directly, civilians forfeit any "protection against attack."[98]

To what extent is the *Tallin Manual* project international, or even a framework for law at all? The non-binding rules composed by the CCDCOE's "International Group of Experts" rely principally on the military manuals of Canada, Germany, the UK and the US. Although its authors argue that these documents form the basis of the "international legal community's" body of opinion on "conflict issues," the specific utility to NATO is quite plain.[99] *The Tallin Manual*, with origins in the US Naval War College, adapts certain aspects of the contradictory concept of humanitarian war and applies these standards to all states in their conduct when using new technologies. Outside of perfunctory consultation with the Red Cross, the manual's rules are subject to no independent adjudication. There is no pretense to formal legislative, let alone democratic input. The rules as such largely preserve the plausible deniability that is a central advantage of cyber warfare, and the authors even describe the manual itself as a mere opinion of experts acting in a "private capacity"; they can therefore make no claims to consistency. These documents then consist of a set of competing rationales, which will undergo successive revision. In context, their use must be seen as political rather than legal, and international only as far as any US-led NATO publishing endeavor can be.

88 Sponsors are listed at the following site: https://cycon.org/cycon2021/sponsors.html.
89 Schmitt later edited its proceedings, published in *Naval War College International Law Studies*.
90 Further biographical information for Schmitt may be found at the website of the Harvard Law School Program on International Law and Armed Conflict: https://pilac.law.harvard.edu/michael-n-schmitt/.
91 Kalev Leetaru, "What Tallinn Manual 2.0 Teaches Us About The New Cyber Order," *Forbes*, 9 February, 2017. Notably, the *Tallinn Manual 2.0*'s subtitle was altered from that of the first edition to apply to "cyber operations," rather than "cyber warfare," an indication of its expanded attention to activities falling beneath threshold of armed conflict.
92 The Tallinn Manual 3.0 Project: https://ccdcoe.org/research/tallinn-manual/
93 The text of the introduction to the *Tallinn Manual* can be found at the following link: https://www.cambridge.org/catalogue/catalogue.asp?isbn=9781107024434&ss=exc
94 Michael N. Schmitt (ed.), *Tallinn Manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University Press, 2013), pp. 53-4. Further information on the *Tallinn Manual 2.0* may be found here: https://ccdcoe.org/news/2017/tallinn-manual-2-0-on-the-international-law-applicable-to-cyber-operations-to-be-launched/.
95 Schmitt (ed.), *Tallinn Manual*, 3.
96 Ibid., pp. 30-1, 34.
97 Ibid., 106.
98 Ibid., pp. 112, 118, 184.
99 Ibid., 8.

CYBER EXERCISES

Central to the CCDCOE's activity is its organization of the regularly-occurring exercises Crossed Swords and Locked Shields. The former was first launched in 2016 as a so-called "red teaming" exercise, meaning participants simulate cyberattacks. According to CCDCOE, Crossed Swords tests the ability of national cyber commands, special forces and military police to plan and execute a "full-scale cyber operation."[100] Since 2018, the exercise has expanded considerably, and now comprises a "cyber-kinetic" engagement of military units – that is, the domain of cyber warfare that may inflict real damage on infrastructure or personnel, as traditional weapons do.[101] Such drills plainly exceed the purely defensive purpose connoted by the CCDCOE's official mission.

NATO and EU cyber exercises

Selected. The EU and NATO organize many more such exercises independently or jointly.

CYBER COALITION: NATO's largest annual cyber defense exercise.[102]

Crisis Management Exercise -CMX: Annual exercise involving both civilian and military staff in Allied capitals. It combines civil and military scenarios.[103]

Cyber Europe: Simulations of large-scale events escalating to crisis. Organized regularly by ENISA (European Union Agency for Cybersecurity) for both public and private sectors. Drawn from EU and EFTA member states.[104]

EU Cybrid: Strategic cyber defense exercise jointly organized by the Estonian Presidency of the Council of the European Union, the Estonian Ministry of Defense and the European Defence Agency (EDA) in 2017.[105]

Parallel and Coordinated Exercise - EU PACE: Large civil-military exercise staged by the European Union. Participating officials drawn from the European Commission, the European External Action Service (EEAS), General Secretariat of the Council, EU member states, other EU agencies.[106] In 2017, participants of EU Cybrid and EU PACE were confronted with the following scenarios or adversaries: regular cyber-attacks, the circulation of "fake news," immigrant trafficking, religious terrorist sects, and an anti- globalization group whose protests are funded by an enemy state.[107]

Coalition Warrior Interoperability eXploration, eXamination, eXercise -CWIX: Largest "interoperability" event of its kind within NATO.[108]

PACE, CMX and Multi-Layer Crisis Management Exercise 2018: Drill for cooperation of EU and NATO; initiated by Joint Declaration of EU and NATO of 6 December 2016.[109]

100 Exercise Crossed Swords 2020, https://ccdcoe.org/news/2020/exercise-crossed-swords-2020-reached-new-levels-of-multinational-and-interdisciplinary-cooperation/.
101 Crossed Swords, CCDCOE: https://ccdcoe.org/exercises/crossed-swords/
102 NATO press release "Exercise Cyber Coalition 2020", 16 November 2020, see: https://shape.nato.int/news-releases/exercise-cyber-coalition-2020.
103 "Crisis Management Exercise 2017," NATO Press Release, see: https://www.nato.int/cps/en/natohq/news_147373.htm.
104 EU Agency for Cybersecurity (ENISA) list of publications and overview: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.
105 "First cyber exercise at EU ministerial level focuses on strategic decision-making," European Defence Agencey, 07 September 2017, see: https://eda.europa.eu/news-and-events/news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making.
106 "Crisis preparedness: EU launches civil-military crisis management exercise," European Union External Action Service, 16 November, 2018. https://eeas.europa.eu/headquarters/headquarters-Homepage_en/53926/Crisis%20preparedness:%20EU%20launches%20civil-military%20crisis%20management%20exercise.
107 Answer of the German Federal Government to parliamentary question, "Cyberübungen der EU und der NATO und ihr mögliches Überschreiten der Schwelle eines bewaffneten Angriffs," 31 July, 2017: https://dserver.bundestag.de/btd/18/132/1813271.pdf.
108 "Federated Interoperability," Statement of the NATO Allied Command Transformation. See: https://www.act.nato.int/federated-interoperability
109 NATO Press Release 6 December, 2016. https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

The annual exercise Locked Shields, organized and hosted by CCDCOE since 2010, is now one of the world's largest cyber military drills. Locked Shields enlists participants from groups called Computer Emergency Response Teams (CERTs, or military CERTs) to train in ostensible defense of information systems and critical infrastructure. According to the CCDOE, the drill's "focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects."[110] The number of participants in recent years has ranged from 1000 and 1500. Aside from academics, delegates from militaries, defense ministries and police agencies (including the FBI) as well as journalists are party to this war game; they are invited to impersonate themselves, as it were, in order to lend authenticity to the simulation.[111]

Private commercial interests participate in these war simulations on more than an episodic basis. For example, CCDCOE has established formal contractual relationships with a number of global firms such as Siemens, which allows for the use of firms' hardware and software.[112] In 2020, CCDCOE and Siemens signed a memorandum of understanding formalizing their cooperation: the think tank will use the firm's technology over the course of the annual Locked Shields simulations, and Siemens will in turn exploit these events to study its own systems' weaknesses.[113] Other companies also contribute infrastructure: one sponsor from the ROK supplies water purification stations; the telecom operator Elisa has set up a special broadband network for the simulation; and Bittium, a Finnish security and medical technology firm, has supplied communications equipment.[114]

In the Center's 2021 drill, "blue team" – or defensive – participants simulated repelling cyberattacks and disinformation which had targeted a NATO state's critical infrastructure, a scenario which tested the framework of NATO's 2016 resolution to treat cyberattacks as worthy of retaliation by the alliance as a whole under Article V's provision for "collective defense."[115] In the scenario, "red team" Crimsonia attacked the state of Berylia's financial sector, mobile networks and water supply. According to NATO's deputy secretary-general Mircea Geoană, the combination cyberattacks and disinformation in this year's simulation was understood as a response to Russia and China, which, Geoană alleged, had attempted to use the Covid-19 crisis to exploit vulnerabilities and to "sow seeds of doubt and discord."[116]

In recent years, scenarios for CCDCOE drills have included the simulation of attacks on a military airport, energy supply systems and central computer networks, vandalism of websites, dissemination of false reports, data theft, commandeering of military drones and the control of airplane refueling systems.[117] In 2019, CCDCOE simulated the circulation of fake news and disinformation, which, by "sowing doubt," incited a domestic population. Blue, defensive, teams were tasked with countering these incursions through use of social and traditional media channels.[118]

STAFF AND AFFILIATIONS

The CCDCOE's steering committee, its executive body, takes all administrative, policy and operational decisions, and oversees the Center's budget and development as well as the CCDCOE's program. All sponsoring states are represented on it, and non-NATO members may be included as contributing participants. It is chaired by a representative of Estonia, the host country, but its individual members are not disclosed. The personnel working in the six branches of the think tank (technology, strategy, operations, law, education/training, support) may be recruited from the Center's sponsoring states. At present, the Center employs twenty-four researchers, advisers and administrative staff, including the director. The composition of CCDCOE staff is both military and civilian, and is populated by German, Portuguese, Japanese, Hungarian and Croatian officials, though a majority are Estonian. The CCDCOE also uses the honorific "ambassador" to refer to former staff who continue to be affiliated with it; "senior fellows" are those who have "developed a special relationship with the CCDCOE" and who are

110 CCDCOE info on Locked Shields: https://ccdcoe.org/exercises/locked-shields/.
111 Thomas Schimmeck, a German radio journalist, contributed a mock radio component to the 2018 drill, despite being a recognized conscientious objector. He was tasked with drafting newspaper articles for both belligerents, on offensive and defensive sides. See Thomas Schimmeck, "Mein erster Cyberkrieg. Die NATO probt den Ernstfall," *NDR, 2 February, 2018*:
https://www.deutschlandfunkkultur.de/die-nato-probt-den-ernstfall-mein-erster-cyberkrieg.3720.de.html?dram:article_id=403011.
112 "Know the CCDCOE: Interview with Director Col. Jaak Tarien," NATO Association of Canada, 29 January, 2020: https://natoassociation.ca/know-the-ccdcoe-interview-with-director-col-jaak-tarien/.
113 Siemens Press Release, "Siemens und NATO CCDCOE vertiefen Zusammenarbeit bei Cyber-Sicherheit für kritische Infrastrukturen," 1 July, 2020: https://press.siemens.com/global/de/pressemitteilung/siemens-und-nato-ccdcoe-vertiefen-zusammenarbeit-bei-cybersicherheit-fuer.
114 "Know the CCDCOE: Interview with Director Col. Jaak Tarien", NATO Association of Canada, 29 January, 2020, https://natoassociation.ca/know-the-ccdcoe-interview-with-director-col-jaak-tarien/.
115 "Cyber defence," NATO web page, 2 July 2021: https://www.nato.int/cps/en/natohq/topics_78170.htm.
116 Shannon Vavra, "NATO tests its hand defending against blended cyber-disinformation attacks," *Cyberscoop* 19 April, 2021:
https://www.cyberscoop.com/nato-blended-cyber-disinformation-defense-locked-shields-article-v/
117 See answer to parliamentary inquiry, "Cyberübungen der EU und der NATO und ihr mögliches Überschreiten der Schwelle eines bewaffneten Angriffs," Question No. 11, 31 July, 2017:
https://dserver.bundestag.de/btd/18/132/1813271.pdf.
118 See answer to parliamentary inquiry, "Aktivitäten der Bundesregierung gegen illegitime Beeinflussung demokratischer Willensbildung," Question No. 28, 19 August, 2019:
https://dserver.bundestag.de/btd/19/124/1912489.pdf.

"committed to supporting its activities on a continuing basis."[119] Both positions index the expansion of the Center's institutional network, which now extends to OECD countries outside of the North Atlantic.

Thomas Svensson, currently the CCDCOE's sole senior fellow, is also national security deputy at the Swedish Telia Company, a telecommunications firm and mobile network provider across Scandinavia and the Baltic (it operates in Sweden, Finland, Norway, Denmark, Lithuania, Latvia and Estonia). A Swedish national and veteran of his country's army, Svensson is also member of several NATO groups focused on tactical communications (TACOMS) and their use in the US and Europe. He has been a consistent participant in the CCDCOE's Locked Shields exercise. All four current CCDCOE ambassadors are likewise drawn from military, intelligence, cyber security and law backgrounds, and reinforce linkages between the Estonian center and Atlanticist circuits in academia and the state.

Prominent among the Center's "ambassadors" is Kenneth Geers, who has operated for years across US intelligence and military positions at the NSA and US Navy, and was a "global threat analyst" at FireEye, a publicly traded cybersecurity company based in Santa Clara County, California. Geers is currently a senior research scientist at COMODO, another commercial cybersecurity group. He is a non-resident senior fellow at the Atlantic Council's Cyber Statecraft Initiative, an affiliate with the Digital Society Institute-Berlin, and a visiting professor at Taras Shevchenko National University of Kyiv, Ukraine,[120] in addition to being active in publishing, editing and publicizing cybersecurity matters related to the CCDCOE.[121] In July 2020, for example, he spoke at the Younger Generation Leaders Network meeting organized by NATO's Public Diplomacy Division, where he addressed "Cybersecurity and its impact on transatlantic security relations and nuclear risks."[122]

Also well connected to industry and government is the CCDCOE's former director Merle Maigre. Before her directorship, Maigre was security adviser to Estonia's president, worked in the policy unit of the NATO secretary general's office and headed NATO's liaison to Kyiv. In the NATO department of Estonia's ministry of defense, Maigre was tasked with preparing the country's accession to the alliance. After only a year at CCDCOE, she took up a position as the chief lobbyist for CybExer Technologies, an Estonian security firm which now contracts directly with NATO and is rapidly expanding its activities in Estonia, Luxembourg and Ukraine. The firm profits from a longstanding collaboration with CCDCOE as a contributor to the latter's exercise Crossed Swords, and specializes in the simulation of offensive and retaliatory operations.[123] Characteristically, Maigre is also linked to Atlantic-oriented think tanks: she was previously a Ron Asmus Fellow at the German Marshall Fund in the US, and was a non-resident transatlantic fellow at the GMF's Warsaw Office.[124]

OUTPUT, MEDIA AND IMPACT

The Center published a dozen reports in 2019, and doubled its output in 2020. This mix of books, articles and conference proceedings also includes reports on recent alleged cyber "events," and generally reflects the Center's four branches of research and activity – technology, strategy, law and operations. In its publicity, the CCDCOE has added to its portfolio a regular brief on these developments and their military implications; it has published eleven such reports since spring 2020.[125] Although this brief is aimed explicitly at the NATO military command, its material also addresses the wider public. In its first number of April 2020, CCDCOE warned of the potential cyber risks due to the increase in remote working. The report was taken up by several media outlets. Jaak Tarien, director of CCDCOE, for example, was quoted by the AFP in October 2020, where he warned that "large scale use of remote work has attracted spies, thieves and thugs"; defensive measures would require greater investment of resources and a new approach. Tarien was, furthermore, convinced that the public only sees a fraction of "the magnitude of malicious activities taking place in the Covid-era busy cyberspace."[126] NATO also rang the alarm in press release.[127] Unsurprisingly, the CCDCOE brief of April 2020 was quick to associate the alleged emerging cyber threats

119 CCDCOE Senior Fellows: https://ccdcoe.org/about-us/
120 ESMT Berlin faculty page: https://faculty-research.esmt.berlin/institutes/digital-society-institute/meet-our-team; Kenneth Geers, Academia.edu profile: https://univ-kiev.academia.edu/KennethGeers
121 The Atlantic Council page for Kenneth Geers: https://www.atlanticcouncil.org/expert/kenneth-geers/
122 European Leadership Network page: https://www.europeanleadershipnetwork.org/networks/ygln/ygln-network-meetings/2020-2/
123 "Director of NATO Cyber Centre in Tallinn Merle Maigre to join the CybExer Team," 16 August, 2018. See: https://cybexer.com/news/director-of-nato-cyber-centre-in-tallinn-merle-maigre-to-join-the-cyb-exer-team/; and "Merle Maigre assumes command of NATO CCDCOE," 31. August 2017 CCDCOE Release: https://www.ccdcoe.org/news/2017/merle-maigre-assumes-command-of-nato-ccdcoe/
124 Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO," Policy Brief GMFUS, 12 February, 2015 https://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato.
125 See for example, "Recent Cyber Events and Possible Implications for Armed Forces," CCDCOE April 2020: https://ccdcoe.org/uploads/2020/05/Recent-Cyber-Events-and-Possible-Implications-for-Armed-Forces-1-April-2020_Final.pdf
126 "Cyber warriors sound warning on working from home," *AFP*, 14 October, 2020: https://www.france24.com/en/20201014-cyber-warriors-sound-warning-on-working-from-home
127 "Cyber Crime Amidst Covid-19 Threat," 20 March, 2020 NATO Press Release: https://shape.nato.int/news-archive/2020/cyber-crime-amidst-of-covid19-threat-countering-malicious-activities.

of the Covid-19 period with Russian disinformation, and ostensible Russian efforts to divide NATO.[128]

It is evident that these warnings are one component of a specific storyline aimed at the public: the world is dangerous, even and especially on the internet, and most of its lurking villains are to be connected to Russia. Civil society must be prepared. Yet it is the CCDCOE which works as part of NATO to transform the internet into a domain of offensive military operations. Already in December 2017, NATO's secretary general Jens Stoltenberg announced the features of the alliance's strategy that will pertain to cyberspace. Stoltenberg indicated that, just as with its air and naval weapons, NATO will use digital technology's offensive capacity. His remarks signaled an official shift from NATO's professed defensive to offensive use of this technology, which had in any case been long in the making, as is illustrated by the exercise scenarios and other activity undertaken by CCDCOE since its founding.[129]

THE STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE (STRATCOM COE)

The NATO Strategic Communications Centre of Excellence (Stratcom CoE) is a Latvian-based think tank founded in the fall of 2014. It is one component of NATO's ramped-up hybrid warfare program, and is devoted to the study and promotion of "strategic communications," or the coordination of diplomatic and public relations, as well as information and psychological operations – that is, NATO's propaganda efforts. The antecedent to its founding was the 2011 reduction in NATO occupation forces under its command in Afghanistan, which was determined by internal NATO analysis to have been weakened by a failure of communications in large part. NATO's self-critical report, written by retired Canadian colonel Brett Boudreau, found that "by the end of December 2014, and still as of December 2015" there was "no Allied joint doctrine manual on StratCom" and only a "conflicting or confusing" set of policies with respect to it.[130] NATO's 2014 Wales Summit thus initiated a renovation of its strategic communications, for which the Riga center was founded as one element.

The Riga Stratcom CoE runs on a modest annual budget of just under €600,000, and takes as its main focus "research and analysis, concept development, experimentation, as well as education and training." In its first year of operation, 2014, it was assigned the task of studying "Russia's information campaign against Ukraine"; with Arizona State University, it undertook a study of ballistic missile defense, and administered training "for Ukrainian and Georgian Government representatives." In 2014, through a seminar on the "Weaponisation of Social Media," the Center produced an assessment of the use of the military in social media, reflecting NATO propaganda's reorganization around the increased velocity and new structure of interaction with the public then characterizing developments in military communication.[131] Boudreau's critical report on NATO's Afghanistan mission had produced an outline for the revision of strategic communications, in which the elimination of certain "firewalls" – or divisions between disciplines of military communications – was to take priority. Given technical changes in communication, so the 2014 report argued, emphasis should be placed on integration of the several sub-fields of propaganda, rather than on enforcing their separation. Public affairs and psychological operations, foreign and domestic audiences, public affairs and information operations, political and military domains: these previously distinct spheres of activity would now be brought under joint control. In sum, this meant that distinctions between psychological operations designed to manipulate audiences with ostensibly truthful representations, and the "value neutral" dissemination of information that is the realm of public affairs, might be formally abolished, as would any distinction between foreign and domestic addressees. As Boudreu put it, "[t]he foreign/domestic audience separation is a faulty foundation on which to base organisational structure any more [sic]."[132] Likewise, untruthful statements, or the deliberate use of false information – the practice of information operations (InfoOps) – was now also to be conjoined with "public affairs." The stated rationale for this was improved rigor in screening for the misuse of untruthful information in the latter; but the practical reality of this bureaucratic reorganization must be understood as effecting the formal abolition of separations between the offices using false information, and those officially devoted to informing the public truthfully. The Boudreau report furthermore

128 "Recent Cyber Events and Possible Implications for Armed Forces #1," CCDCOE Report, April 2020: https://www.ccdcoe.org/uploads/2020/05/Recent-Cyber-Events-and-Possible-Implications-for-Armed-Forces-1-April-2020_Final.pdf

129 Stoltenberg: "What we're doing is defensive, but we need to develop our capabilities." An *FAZ* correspondent's interpretation: "Now it's becoming clear that it's heading in the direction of offensive weaponry." See Constanze Kurz, "Cyber-Strategie der Nato: Auf den Schlachtfeldern der Zukunft," *Frankfurter Allgemeine Zeitung*, 11 December, 2017. See also the CCDCOE paper by Alzbeta Bajerova, "Impact on NATO of Cyberspace as a Domain of Operations," SWOT Analyses, 2017.

130 Brett Boudreau, "We Have Met the Enemy and He Is Us: Analysis of NATO Strategic Communications: The International Security Assistance Force (ISAF) in Afghanistan, 2003-2013," (Riga: 2016), p. 343. Boudreau is currently a consultant for Veritas Strategic Communications. See: https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/isaf_full_report_06-04-2016.pdf

131 NATO Strategic Communications Centre of Excellence Annual Report 2014, pp. 3-4.

132 Boudreau, "We Have Met the Enemy and He Is Us," 282.

recommended an elimination of the division of political and military public affairs, so as to liberate NATO military personnel from strictures on directly political interventions. Such activity had already been pioneered by an active duty officer's diplomatic visit to Pakistan, but at the time it was of dubious permissibility. The new regulations supported by Stratcom would clarify that such practices were not only permitted, but encouraged.[133]

Boudreau's "We Have Met the Enemy, and He is Us" is the foundational document for the Stratcom COE, and charts the perspective of the think tank: it prizes the fusion of civilian and military structures within NATO, is indifferent as to whether it addresses foreign or domestic publics, and in its conceptualization of NATO communications, merges information operations and psychological warfare with public relations. These innovations in military communications are justified on the basis of safeguarding truth, but in practice they rely on the collapse of previously segregated departments within the military command, and exploit a new media environment which is virtual, instantaneous, automated and interactive.

STRUCTURE

The Center consists of four branches devoted to "doctrine, concept and experimentation, education and training, operational support and framework nation support." As with other NATO Centers of Excellence, it is governed by a steering committee, which meets biannually, and which is presided over by a Latvian national. Since 2015, the Center has operated under the directorship of Jānis Sārts, drawn from the Latvian Ministry of Defence, and is chaired by its former spokesman Kaspars Galkins. Its deputy director, Peeter Tali, is an officer in the Estonian military. In recent years, the Center's membership has expanded to include – in addition to the original Baltic founding states plus Germany, Italy and the UK – the Netherlands, Finland, Sweden and Canada. French and Slovakian accession is planned for the near future. Along with conference-hosting obligations and the development of NATO's communications doctrine, the Center publishes a bi-annual, peer-reviewed, journal, *Defence Strategic Communications* (DSC), edited by Neville Bolt of King's College, London. The journal's editorial board is comprised of professors from the Baltic states, the UK, Brazil, Georgia and Japan, and publishes articles by an international roster of contributors.

OUTPUT

The substance of Stratcom's output is to be found in this in-house journal, *Defence Strategic Communications*. Its contents reveal much about the framework of NATO's new strategic communications and propaganda footing. In DSC's 2016 inaugural issue, two exemplary articles especially merit scrutiny. "The Narrative and Social Media," written by US Army Psychological Operations Specialist Miranda Holmstrom, offers an especially stark framing of the contemporary media environment, and NATO's activity within it. A second, "It's Time to Embrace Memetic Warfare," by the right-wing US-American activist, Thiel Capital and Softbank-backed financier Jeff Giesea, demonstrates that Stratcom has openly considered, from its founding, plans for the active, rather than merely defensive use of disinformation.

Holmstrom's "The Narrative and Social Media" is a set of considerations on new mode of "winning hearts and minds" by way of "harness[ing] the power of social media" to promote "simple yet complete narratives that can easily be reproduced."[134] Holmstrom understands narrative – "a framework for the plot and setting of a story" – as a fundamental tool of "propaganda," because it is a form of sense-making through which the density of information may be mentally shaped and remembered. Such efforts will focus on the individual "as a member of a group," and will be public in nature:

In the sphere of StratCom for the defence community the narrative is a framework of [sic] creating or reinforcing opinions as well as collective beliefs and transforming them into action.[135]

Narratives, Holmstrom, contends, may even work to foster an irrational response to a given set of events. They furthermore introduce a "problem," which requires a solution – much as in the structure of the *fabula* in a work of fiction, propaganda narratives use "set-up, conflict, resolution" to guide thinking and action of their targets. Indeed, given the artificiality of its structure, the truth itself in such a form, is found "not in its verifiability, but in its verisimilitude – the appearance of it being real or true."[136]

133 Ibid., pp. 283-84.
134 Miranda Holmstrom, "The Narrative and Social Media," *Defence Strategic Communications* Vol. 1 (March 2016), 119.
135 Ibid., pp. 120-2.
136 Ibid., 123.

Social media, for its, part, according to Holmstrom, favors "horizontal propaganda" – which develops laterally through individual-to-individual contact, in contrast to the "vertical propaganda" of a traditional marketing operation. Such "horizontal" propaganda solicits activity and participation, and "creates the illusion of choice, free will and personal decision-making" to achieve compliance. Holmstrom concludes that "[i]n the battlefield of narratives, merely telling the truth is not effective enough."[137]

What might such horizontal propaganda look like in practice? The answer is partially given in Jeff Giesea's short article in the same number of *Defence Strategic Communications*. Giesea advises using fake accounts to mislead users of social media. He recommends "more aggressive communication tactics and broader warfare through trolling," and enjoins NATO to boost its capacity for waging "memetic warfare" – or information operations "tailored for social media" in which the stakes are "narrative and idea" and "social control in a social-media battlefield."[138] Giesia, concerned that NATO strategic communications were then in 2016 "tepid, timid, and stale," and "Version 1.0 of a software program," advocated "experimentation" and "guerilla efforts" requiring more funding and personnel devoted to information operations. Generals must become active on Twitter, Giesia argued, if social media is to be fully exploited, as is necessary, and legal and ethical hurdles would have to be overcome.[139]

Articles appearing in later volumes reflect Giesia's early focus on social media. Two articles from later volumes in 2016, "Internet Trolling as a Tool of Hybrid Warfare," and "Social Media as a Tool of Hybrid Warfare," both argue that the presence of Russian and ISIS internet commenters on social media necessitates greater "filtering" by the leading firms, to "automatically delete comments" and to "develop unifying narratives" favorable to NATO.[140] The second of these two reports does not recommend censorship, but rather a "heightened social media presence," and argues that "lack of engagement in social media is no longer an option."[141] Although ostensibly defensive in nature, such actions are indistinguishable in practice from the aims of hybrid warfare itself, and in scale – given the ownership structure of the major global social media firms, the largest of which are based in the US – are far more consequential, especially when set in the context of Giesea's recommendations and what is publicly known about NATO and the US's own active disinformation efforts.[142] The extent to which Stratcom takes an interest in private firms' own software is indicated by a 2020 contribution by Henrik Twetman, Marina Paramonova, Monika Hanley, "Social Media Monitoring: A Primer," in which the various media platforms are evaluated based on the ease with which their internal tracking can be accessed freely. The report evaluates the extent to which API, or "application programming interfaces"[143] may be used to track usage of platforms. It references the Atlantic Council's Digital Forensic Research Lab, which has developed its own tools for this end, and which also relies on Facebook's own tracking mechanism, called CrowdTangle.[144] For a separate report on "Social Media Manipulation," Stratcom "partnered with US Senators Chuck Grassley...and Chris Murphy," to buy interactions on each of their accounts in order to test the capacity for small payments to drive responses to the activity of public figures. The report concluded that governments must "pressure social media platforms" to tighten their policing of social media use, given the "striking" level of "openness of [the] industry."[145]

137 Ibid., pp. 126, 131.
138 Jeff Giesea, "It's Time to Embrace Memetic Warfare," *Defence Strategic Communications* Vol. 1 (March 2016), pp. 67-9. Giesea: "Cyber warfare is about taking control of data. Memetic warfare is about taking control of the dialogue, narrative, and psychological space."
139 Ibid., 71. "Where is the innovation? Where is the war-gaming of tactical successes at the Strategic Communications level?"
140 "Internet Trolling as a Tool of Hybrid Warfare," *Defence Strategic Communications* (January 2016), 82.
141 "Social Media as a Tool of Hybrid Warfare, *Defence Strategic Communications* pp. 40-1.
142 See for example "Revealed: US spy operation that manipulates social media," *The Guardian* 17 March 2011, and "Can NATO Weaponize Memes?" *Foreign Policy* 13 April 2017.
143 An application programming interface (API) is a layer of code which mediates between an application and a web server, or between two pieces of software. An API may be as simple as a universal login. The type of API referred to here is one which allows third parties to monitor, to varying degrees, the data produced and collected by a particular platform.
144 "Social Media Monitoring: A Primer," *Defence Strategic Communications* (December 2020), p. 28.
145 "Social Media Manipulation 2020: How Social Media Companies are Failing to Combat Inauthentic Behaviour Online," *Defence Strategic Communications* (November 2020), pp. 8-9, 15.

A 2020 contribution to DSC, "Deepfakes – Primer and Forecast" by Tim Hwang, focused on technical innovations of visual disinformation and the use of artificial intelligence in creating convincing false images and video. Hwang, a science and technology writer formerly of Google, MIT Media Lab,[146] MIT-Harvard AI Initiative and RAND, is now at the Center for Security and Emerging Technology at Georgetown. Hwang himself participated in at least one social media-oriented experiment in strategic communications funded by the US's Defense Advanced Research Projects Agency (DARPA), in 2016.[147] The contribution combines both technical overview of increasingly convincing fake images and video, and, as a matter of policy advice, recommends "building connections with the technical media forensics community" and "supporting research on the psychological dimensions of deepfakes."[148]

MEDIA

Stratcom has enjoyed popular media coverage of some of its exercises and reports. A profile in *Politico* in March 2016, described it as on the "front lines of the palpably intensifying information war" with Russia, and featured words of encouragement from a retired Marine attaché at the US embassy in Riga.[149] A 2018 "red team" test undertaken in cooperation with the Cooperative Cyber Defence Centre of Excellence (CCDCOE), in which members of NATO militaries were tracked and manipulated online, saw a writeup in *Wired*, and featured prominent commentary from Stratcom director Jānis Sārts, and the study's author Sebastian Bay ("we need to put more pressure on social media").[150] In the spring of 2021, Stratcom's reports on social media were covered by the German English-language state broadcaster *Deutsche Welle*.[151] The Center has also been boosted in the Atlantic Council's own blog, *The New Atlanticist*.[152] In addition to frequent coverage in local Latvian media, the Center's reports have also been picked up by the Associated Press, and carried in small markets within the United States; the Center's publications and history has also been publicized in the *Frankfurter Allgemeine Zeitung* and *El País*.[153]

The flattering international coverage in some of the most prominent outlets of NATO societies holds in relief one consistent feature of NATO's strategic communication: it is built around the message of a foreign threat, but at no time since the Cold War has consolidation around NATO's adversaries been so consistently regulated and enforced culturally. It is from the pulpit of *El País* that Sārts warns of incursions by "Russia, China and Iran" into the West, and where he anticipates foul play in upcoming German and French elections. But the basis of these alarms is Stratcom's own simulations of social media influence, with little to show for any pro-Russian, let alone Chinese or Iranian effect anywhere in the NATO and other US-allied countries, where most publics have favorable views of Merkel and Biden, and highly negative views of Xi and Putin.[154] Stratcom's warnings themselves conform to a disciplined program, now years in the making, in which threats from the east form the horizon of foreign policy. Set in the context of NATO's and specifically US's campaign of stated strategy of confrontation with Russia and China, these efforts should be understood as part of general framework guiding public opinion, rather than responses to the actions of foreign states, as the admiring Western media portray them.

146 The MIT Media Lab is a degree-conferring department within the Massachusetts Institute of Technology, headed founded and directed for years by architect Nicholas Negroponte, brother of John Negroponte, Ronald Reagan's ambassador to Honduras, and, under George W. Bush, ambassador to Iraq (2004-05), and director of national intelligence.

147 See V. S. Subrahmanian et al., "The DARPA Twitter Bot Challenge," *Computer*, Vol. 49, No. 6, June 2016. From the abstract: "DARPA held a 4-week competition in February/March 2015 in which multiple teams supported by the DARPA Social Media in Strategic Communications program competed to identify a set of previously identified 'influence bots' serving as ground truth on a specific topic within Twitter."

148 Tim Hwang, "NATO Deepfakes: A Primer" *Defence Strategic Communications* (May 2020), pp. 21-22.

149 See Gordon F. Sander, "Latvia's fortress think tank," *Politico* 16. March 2017.

150 Issie Lapowsky, "NATO Group Catfishded Soldiers to Prove a Point about Privacy," *Wired*, February 18, 2019. For the study itself, see Sebastian Bay et al., "Camouflage for the Digital Domain: A Force Protection Framework for Armed Forces," *Defence Strategic Communications* (February 2020), *passim*.

151 "How social media is manipulated – and how Russia is involved," *DW,* 14 April 2021: https://www.dw.com/en/how-social-media-is-manipulated-and-how-russia-is-involved/a-57206840

152 See Rihards Kols, "NATO Must Meet Russia's Hybrid Warfare Challenge" (3 July, 2018): https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-meet-russia-s-hybrid-warfare-challenge/

153 "NATO report says social media account manipulation affects even US senators," *Associated Press*, 22 December, 2020. The story was picked up by, for example, a small Arkansas newspaper, the *Sentinel Gazette*. See also "Wir haben es mit medialem Krieg zu tun," *FAZ* 29 January, 2017 and "El manejo de los datos será en el futuro una amenaza a la seguridad nacional," *El País* 7 July 2021, in which Sārts was profiled.

154 See Pew Research Center Report of 9 June, 2021: https://www.pewresearch.org/global/2021/06/10/americas-image-abroad-rebounds-with-transition-from-trump-to-biden/pg_2021-06-10_us-image_00-09/

GLOBSEC

GLOBSEC, a Bratislava-based think tank established in 2005, is the successor to the Slovak Atlantic Commission, founded in 1993 to support Slovakia's accession to NATO.[155] Unlike the think tanks previously discussed in this study, GLOBSEC does not belong to the NATO Centers of Excellence network. It is thus not overtly geared toward training the military and national security apparatuses of NATO states, but rather addresses civil society more broadly, particularly in central and eastern European countries where it aids in NATO's consolidation and potential expansion, and integrates central European elites into the circuits of transatlantic power.

This "global think tank," according to the EU transparency register, is an "independent, non-partisan, non-governmental organization"[156] focused on shaping foreign and security policy. To this end, GLOBSEC organizes a number of annual conferences and cooperative projects, and publishes on strategy within the GLOBSEC Policy Institute. Its research is divided into five departments: Defense & Security, Energy, the Future of Europe, Strategic Communication and Cyber Security. GLOBSEC representatives meet regularly with EU commissioners, their cabinets, as well as the Commission's directorates-general; in 2020 alone, there were seven such meetings. With regard to EU institutions and policies, GLOBSEC concentrates its activities on the following broad fields: "foreign policy, security and defense, countering hybrid threats and foreign subversive efforts." Among its European and US sources of funding – the European Commission, and the National Endowment for Democracy – two further sponsors are of particular interest: NATO's Public Diplomacy Division and a second rather opaque source listed as "various business entities."[157]

STAFF AND BOARD MEMBERS

The distribution of GLOBSEC's staff of forty-six across its multiple programs suggests a prioritization of their "strategic forums," meaning GLOBSEC's different conference schemes (which employ twelve), and its Policy Institute (with seven employees and thirteen associate fellows).[158] Former Austrian finance minister Wilhelm Molterer and former Polish undersecretary of state treasury Michał Krupiński sit on the executive board, which is mainly comprised of those with banking, government and related backgrounds from Hungary, Bulgaria, Poland, the Czech Republic, Slovakia and Austria. Anita Orbán, the sole woman executive board member, is Hungary's former ambassador for energy security and executive at gas firm Tellurian. She is currently a director at the telecommunications company Vodafone.[159]

Key members of GLOBSEC's international advisory board link it to NATO and US foreign policy establishment circles. Of the twenty-four members of this board, eleven are US citizens with ties to US-based think tanks, its foreign service, military and government. Five of the eleven are affiliated with the Atlantic Council. Among them is Michael Chertoff, former US federal judge and head of Department of Homeland Security from 2005-2009, who is now executive chairman of the Chertoff Group and counsel to governments and corporations on security matters.

Other notable board members at GLOBSEC include:

- Alexander Vershbow, the former deputy secretary general of NATO and US assistant secretary of defense for international security affairs, as well as a former ambassador to NATO as career member of the US Foreign Service.

- Damon Wilson, currently vice president and director of the International Security Program at the Atlantic Council. He is a former special assistant to the president and senior director for European Affairs at the National Security Council.

- Ian Brzezinski (son of Zbigniew Brzezinski), senior fellow at the Scowcroft Center for Strategy and Security at the Atlantic Council. Brzezinski served as deputy assistant secretary of defense for Europe and NATO under George W. Bush, and was responsible for NATO expansion and the coordination of European military contributions to US and NATO operations in Iraq, Afghanistan and the Balkans.

- Sally A. Painter, previously of the defunct US Committee on NATO, which advocated increased US influence through the alliance's expansion. The Committee was founded by Bruce P. Jackson, former vice president for Strategy and Planning at weapons manufacturer Lockheed Martin.

155 GLOBSEC's website: https://www.globsec.org/about/.
156 See the GLOBSEC entry in the EU Transparency Register: https://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=903680223573-18.
157 Ibid. Some indication of these sources is given at GLOBSEC's website, in a list of "partners." Among the many listed are defense industry firms such as General Dynamics and Lockheed Martin, technology firms Google and Microsoft, energy firms, industry associations, chambers of commerce, real estate and financial services firms, along with the US State Department and British Embassy in Bratislava. See: https://www.forum.globsec.org/2021/partners.
158 An overview of GLOBSEC's personnel may be found here: https://www.globsec.org/about/people.
159 Orbán took a doctorate at the Fletcher School of Law and Diplomacy in Boston in 2007. For a complete profile, see: https://www.europeanleadershipnetwork.org/person/anita-orban/ and "Anita Orbán appointed as Vodafone Hungary's new external affairs director," *Budapest Business Journal*, 5 January 2021.

- John R. Allen, president of the Brookings Institution. Allen is a retired four-star general in the US Marines and former commander of NATO ISAF and US forces in Afghanistan. Until recently he served on the German Marshall Fund's Transatlantic Task Force and was a board member at Bundeskanzler Helmut-Schmidt-Stiftung.

PROGRAM

GLOBSEC organizes at least three different recurring conferences: the Tatra Summit, the Château Béla Central European Strategic Forum and the Bratislava Forum.[160] The latter, which is GLOBSEC's largest and which has run continuously for sixteen years, is advertised as the "leading platform in the Central Eastern Europe region and one of the top strategic conferences globally."[161] Its roster of speakers often includes heads of government and state, and other prominent politicians. The 2021 conference, which opened with a digital greeting from the Vatican, hosted Austrian chancellor Sebastian Kurz of Austria, Slovakian prime minister Eduard Heger, and Karel Havlíček, deputy prime minister of the Czech Republic, as well as Slovakian president Zuzana Čaputová and her Polish counterpart Andrzej Duda. Representatives of NATO states such as Canadian minister of defense Singh Harjit Sajjan addressed the forum, as did officials from NATO's bureaucracy itself, like Benedetta Berti-Alberti, head of policy planning for the office of secretary general and Baiba Braže, another high-ranking deputy. Also attending in 2021 were Japanese minister of defense Yasuhide Nakayama and executives of Facebook, Microsoft, Apple, and various private equity and pharmaceutical firms. Three speakers were drawn from GLOBSEC's international advisory and executive board (John Allen, Michael Chertoff, Gordon Bajnai).[162] Among the "partners" for the event were the US State Department, Slovak ministries of foreign and European Affairs and of Defence, NATO, the German Konrad Adenauer Stiftung, the European Regional Development Fund and dozens of corporations, including media, technology and financial firms.[163]

The 2021 forum, organized under the slogan, "let's rebuild the world better," opened with a security-themed panel moderated by the British television journalists Maithreyi Seetharaman and Terry Martin. The dozens of ensuing sessions followed the themes of "democratic renewal and rebuilding trust," "economic growth & recovery," "global Europe in a post-pandemic world" and "tech governance." Two further sessions were devoted to "security for the 21st century" and "resilience and health."

The session "Global Trade – Optimism Restored?" focused on barriers to trade, especially with China, and was held against the backdrop of the June G7 communiqué which had resolved "to jointly counter China's growing economic dominance."[164] Huiyao Wang, formerly of the Brookings Institute and Harvard's Kennedy School of Government, and the founder and current president of the Center for China and Globalization in Beijing, emphasized interdependence in the global economy and the priorities of cooperation in trade.[165]

Two sessions of note focused on Russia. In the first, an interview between US undersecretary of state for political affairs Victoria Nuland and the Moscow correspondent for the *New York Times* ("The United States, Central Europe, and Global Democratic Agenda"), warned of possible further US escalation against Russia, on the basis of claims that the latter has violated human rights and allegations it has interfered in elections.[166] Nuland pledged continued support for the current Ukrainian government, and announced that – along with the EU – the US would impose sanctions on Belarus in response to a recent arrest of journalist Roman Protasevich. Nuland's session was followed by a conversation with chief of staff and campaign manager to Alexei Navalny, titled "Democratic Change in Russia: How to increase the Odds?"

A number of the forum's sessions in 2021 reflected intensified collaboration between the EU and NATO. A discussion between Maroš Šefčovič of the European Commission and Mircea Geoană, NATO's deputy secretary-general, was devoted to the reconceptualization of military "resilience," which

160 The annual two-day Tatra Summit is held in the Tatra mountains at the Kempinski hotel and allows "key governmental and EU decision-makers [to]meet with experts and top business representatives," with a nominal focus on central and eastern Europe. GLOBSEC's "exclusive annual gathering," Central European Strategic Forum is held at Château Béla in southern Slovakia, is a smaller, informal meeting for politicians, lobbyists and academics. https://www.globsec.org/projects/chateau-bela-central-european-strategic-forum-2020/.

161 "About the Forum," GLOBSEC: https://www.forum.globsec.org/2021/about.

162 Among the foundations represented among speakers were the Robert Bosch Foundation, Brookings Institution and the German Council on Foreign Affairs. A list of the speakers can be found here: https://www.forum.globsec.org/2021/speakers. Participants are not listed in full.

163 For GLOBSEC's "partners"– left undefined – see: https://www.forum.globsec.org/2021/partners.

164 The G7 also warned that "China increasingly poses a global security problem." See "Shifting Focus, NATO Views China as a Global Security Challenge," *The New York Times*, 14 June, 2021: https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html.

165 Agenda of Bratislava Forum 2021: "Global Trade – Optimism Restored?" https://www.forum.globsec.org/2021/agenda; and for summaries of the panels, see https://www.forum.globsec.org/2021/key-messages.

166 The former charge is the standard rationale for NATO's humanitarian war since 1999, and the latter has been a favorite of US security services operating within US domestic politics, with little substantiation to back it up, since 2016. For more on Nuland, see page 11 above for discussion of her 2014 commentary on EU-Ukrainian relations, in a period when the US supported the overthrow of the Ukrainian government unilaterally. A transcript of her leaked phone call may be found here: https://www.bbc.com/news/world-europe-26079957.

should now be understood, so the speakers argued, to include those security matters related to climate change, critical infrastructure, supply chains, telecommunications and foreign direct investment. It was under this framework that Šefčovič and Geoană boosted NATO's hybrid and cybersecurity agenda vis-à-vis Russia and China. A related second panel fell under NATO's branded 2030 campaign to make "a strong alliance even stronger."[167] Its panelists – Christopher Heusgen, German ambassador to the United Nations and long-time security adviser to Angela Merkel; Katrina Mulligan of the US Democratic Party-affiliated, arms industry and banker-funded Center for American Progress; and NATO ambassador Baiba Braže – pondered NATO's future development. This was followed by a discussion among the Slovakian, Canadian and Macedonian defense ministers.[168] Together they emphasized an escalating great power competition between the West, Russia and China and warned of the dangers presented by cyber and hybrid technology, now exacerbated by the use of artificial intelligence. The ministers' recommendation was unsurprising: ramp-up NATO's capacity for both defensive and offensive action. Based on the topics of discussion at the 2021 forum, it can be inferred that NATO is readying ever more extensive incorporation of defense contractors into its activities. Canadian defense minister Sajjan assured the audience that NATO will be fortified through an increase in so-called public-private sector cooperation, with which Canada has extensive experience.[169]

NATO 2030: NATO, GLOBSEC AND THE PRIVATE SECTOR

In June 2020, NATO secretary general Jens Stoltenberg launched the NATO 2030 initiative, which has tasked civil society – especially its youth and the private sector –with strengthening the alliance. In its early phase, GLOBSEC hosted six joint NATO-private sector online meetings, held between November 2020 and April 2021. Participants attended to a range of topics: the future of warfare, the private sector's role in NATO, so-called "sustainable defense innovation" and climate change, geopolitical competition and information war, ethics and technology and infrastructure.[170] Just who participated in these meetings and how participants were selected remains undisclosed, and only the agenda for the first meeting of November 2020 has been made available to the public. It reveals a mixture of NATO officials, US and European executives, corporate managers and specialists in applied science.[171]

The NATO 2030 public relations campaign begins from the assumption that "NATO's technological superiority is being challenged by Russia and China" and that these "countries do not share transatlantic values or prioritize the ethical deployment of these powerful technologies." To encourage closer cooperation between NATO and the private sector, NATO claims that the "benefits of well-structured public-private partnerships" are well documented.[172] The key argument for pushing them is that "Russia and China are immune from this strategic distance [between the public and the private sector] and can quickly mobilize and co-opt the private sector to achieve its [sic] objective." Thus, Russia and China enjoy a "comparative advantage vis-à-vis NATO."[173] A second conference in this series focused on cooperation across NATO, for which increased funding for small and medium-sized companies, as well as start-ups, will have to be supported. Records of these meetings indicate that among the priorities was greater integration of NATO and private firms, including personnel exchange between the two, to boost morale.[174] Furthermore, it was determined that the private sector is useful for lobbying politicians to reduce regulation ("proposed regulation is too excessive… as more regulation is not always better regulation"); this meeting was in essence an invitation to private firms to escalate lobbying.[175] A third session illustrated well the expansion of the security concept to cover the professed guardianship of global supply chains threatened by climate change. Such rhetoric is on-message with the promise of a "sustainable transformation" of the military alliance, which has advanced the idea that it will become "greener" by way of a "transition away from fossil fuels."[176]

167 NATO 2030 homepage: https://www.nato.int/nato2030/index.html
168 Respectively, Jaroslav Nad', Harijt Singh Sajjan, Radmila Šekerinska. North Macedonia (formerly Macedonia) is the most recent country to join NATO, which it did in March 2020.
169 For a detailed summary of the 2021 Bratislava Forum sessions 2021 see: https://www.forum.globsec.org/2021/key-messages.
170 "NATO-Private Sector Dialogues focus on NATO 2030 initiative," 2 June, 2021: https://www.nato.int/cps/en/natohq/news_184601.htm.
171 "The Future of Warfare and the Role of New and Emerging Technologies," GLOBSEC Events, 25 November, 2020: https://www.globsec.org/events/the-future-of-warfare-and-the-role-of-new-and-emerging-technologies/#agenda.
172 "Public-private partnership" is the euphemism for public subsidy of private firms. A catalogue of the effects of these arrangements has been compiled by Bankwatch, and can be found here: https://bankwatch.org/public-private-partnerships.
173 "The Future of Warfare and the Role of New and Emerging Technologies," NATO 2030: NATO-Private Sector Dialogues with GLOBSEC, 25 November 2020: https://www.globsec.org/wp-content/uploads/2020/11/Main_policy_takeaways.pdf.
174 "The Private Sector's Contribution to Alliance Security," NATO 2030: NATO-Private Sector Dialogues with GLOBSEC, 21 January 2021: https://www.globsec.org/wp-content/uploads/2021/01/NATO-Private-Sector-Dialogues-with-GLOBSEC-21-Jan-Main-Policy-Takeaways-.pdf.
175 "Transatlantic Cooperation on Ethical Deployment and Governance of New Technologies," NATO 2030: NATO-Private Sector Dialogues with GLOBSEC, 25 March 2021: https://www.globsec.org/wp-content/uploads/2021/04/NATO-GLOBSEC-Dialogue-5-Policy-Takeaways.pdf.
176 "Sustainable Defence Innovation and the Fight Against Climate Change," NATO 2030: NATO-Private Sector Dialogues with GLOBSEC, 11 February 2021: https://www.globsec.org/wp-content/uploads/2021/02/NATO-GLOBSEC-Dialogue-3-Policy-Takeaways.pdf.

On 25 February 2021, the GLOBSEC-NATO 2030 agenda moved to answer the question of how the private sector might contribute to the "weaponization of the information space," and how "storytelling" is altered by digitization. Here again Russia and China were singled out as running networks of disinformation necessitating a redoubled NATO response. GLOBSEC's summary indicates that the focus of this session called for more consistent public-private collaboration. Regarding the weaponization of information, GLOBSEC emphasized as a "key insight" the potential utility for NATO of small and medium-sized enterprises (SME) and civil society organizations (CSO) – which had been, up to the present, overlooked. To remedy this, NATO will loosen constraints on subsidizing them. It was furthermore suggested that NATO might use its Stratcom Center of Excellence in Riga as a venue for collaboration with the private sector; the Center could potentially "engage in enhanced interaction with citizens, including addressing disinformation, and promoting media literacy, and more." The meeting summary indicates that Stratcom became the focus of discussion in its second half. Since NATO is engaged in a competition "to win and retain the hearts and minds of its citizens," methods for improving "NATO's storytelling" must be made more effective, and as a complement to its regular production of non-fiction media, NATO must also develop fiction, for which it will collaborate with studios and publishers to produce films, books and video games.

The delegates also found that NATO should be featured in "popular Hollywood movies or online streaming franchises." Moreover, NATO should enlist a greater number of "creative and unconventional surrogates to deliver [its] story." Improvement of the alliance's image is imperative, and for this it will have to expand its reach throughout the culture industry. Public diplomacy aimed at citizens in NATO states should be prioritized so as to convey its importance to them directly. In this venture, "human-interest and community-based stories," targeting citizens in all allied states were held to be most effective. Still, "tailored communication products" for its websites and social media accounts across local languages would also be necessary to reach the widest possible public.[177]

OTHER PROJECTS AND MEDIA IMPACT

GLOBSEC's portfolio also includes academic projects such as its Envisioning a New Governance Architecture for a Global Europe (ENGAGE) program. For ENGAGE, GLOBSEC cooperates with nine universities and four separate think tanks across the European Union, the UK and Turkey to the end of coordinating a common EU foreign policy.[178] GLOBSEC's Geopolitical Europe (GEOP) also focuses on a "more coherent EU Common Foreign and Security Policy," which is supported by the Jean Monnet Activities of the EU Programme Erasmus+.[179] The Slovak Aid Fellowship Program for Change Leaders integrates Belarusian specialists into the ranks of capitalist management, by assigning them Slovakian mentors – those economists and managers who oversaw the shock liberalization of the 1990s.[180] Separately, GLOBSEC's Supporting Democratization and Reconciliation Process in the Western Balkans may be seen as a publicity arm of NATO's continued eastern enlargement – the alliance absorbed North Macedonia in 2020 – for which the catchword "democratization" distinguishes the West from its adversaries.[181]

177 "The Information Landscape as a Theater of Geopolitical Competition," NATO 2030: NATO-Private Sector Dialogues with GLOBSEC, 25 February 2021: https://www.globsec.org/wp-content/uploads/2021/03/NATO-GLOBSEC-Dialogue-4-Policy-Takeaways.pdf.

178 "ENGAGE – 'Envisioning a New Governance Architecture for a Global Europe,'" GLOBSEC Projects: https://www.globsec.org/projects/engage-envisioning-a-new-governance-architecture-for-a-global-europe/.

179 "GEOPE – 'Geopolitical Europe: Are the EU Member-states Ready for It?'" GLOBSEC Projects: https://www.globsec.org/projects/geope-geopolitical-europe-are-the-eu-member-states-ready-for-it/.

180 One might ask if this project constitutes EU and NATO meddling in the internal affairs of a foreign country, and what the response would be if Russian-sponsored Belarusian economists were tutoring Slovakians. The program is funded by European Union's Horizon 2020 research and innovation program. See "The SlovakAid Fellowship Program for Change Leaders," GLOBSEC Projects: https://www.globsec.org/projects/the-slovakaid-fellowship-program-for-change-leaders-2/.

181 NATO Secretary General Jens Stoltenberg: "[Macedonia's accession] shows that NATO's door remains open for countries that meet NATO standards and that adhere to the NATO values of democracy, the rule of law and individual liberty." See "Macedonia signs accord to join NATO despite Russian misgivings," *Reuters*, 6 February 2019. For GLOBSEC's program, see: "Supporting Democratization and Reconciliation Process in the Western Balkans," GLOBSEC Projects: https://www.globsec.org/projects/supporting-democratization-and-reconciliation-process-in-the-western-balkans/

"GLOBSEC Trends 2021" and "GLOBSEC Vaccination Trends" are among the organization's publications intended for a wider public. Both rely heavily on polling conducted throughout central and eastern Europe, the results of which are presented in press-ready charts. For these publications, GLOBSEC questioned the public on East-West relations, China, NATO and democracy, and concludes that shining a "spotlight on China" must be prioritized, as the PRC's rising influence in the central and eastern European (CEE) region has gone largely unnoticed: Bejing's "vaccine and mask diplomacy" is indexed as a reason not to turn a "blind eye to the country." The report, which credits the US's National Endowment for Democracy with "support," furthermore recommends dismantling the so-called "Kremlin mirage," and advises using the case of Alexei Nawalny as an opening "through which the Kremlin's favorable image can be countered." "Moscow's malign subversive acts in Europe," the GLOBSEC authors suggest, will need to be given more prominent media coverage.[182]

In April 2021, GLOBSEC published "Vaccination Trends: Perceptions from Central and Eastern Europe," the findings of a survey of the CEE countries on attitudes toward Covid-19 vaccines undertaken to gauge Russian influence in the region. The report enjoyed international media coverage in Europe (*BBC*, *Politico*, *Reuters*), North America (*The New York Times*, *CNN*, *Bloomberg*) and Brazil, Israel and Japan.[183] In its focus on the geopolitical dynamics of vaccine distribution, it found "that among those willing to be vaccinated, only 1 percent of Poles and Romanians and 2 percent of Lithuanians would choose Sputnik over American or European brands" but that in Slovakia, around fifteen percent preferred the Russian. The *New York Times* interpreted these data as a sign of "political turmoil," because Russia's diplomacy – the donation of 200,000 doses of its brand of vaccine – was "dividing politicians across Europe" and showed that there could be "negative side effects for a recipient country."[184] Few instances could better illustrate GLOBSEC's central function of integration, consolidation and mediated framing of Atlantic power at NATO's eastern border.

182 "Central & Eastern Europe one year into the pandemic," GLOBSEC Trends 2021, June 2021, pp. 76-77: https://www.globsec.org/wp-content/uploads/2021/06/GLOBSEC-Trends-2021_final.pdf.

183 "GLOBSEC Vaccination Trends: Perceptions from Central & Eastern Europe Going Global – media outreach," GLOBSEC News. The vaccination trends report also indicated it had received support from the National Endowment for Democracy: https://www.globsec.org/news/globsec-vaccination-trends-perceptions-from-central-eastern-europe-going-global-media-outreach/.

184 "Russian Attempts to Expand Sputnik Vaccine Set Off Discord in Europe," *New York Times* 2 May, 2021.

CONCLUSION

The apparent return of great power rivalries, especially as articulated by the military and intelligence agencies within the United States, suggests superficially that a new cold war is underway. FBI warnings of US universities infiltrated by Chinese students, of elections and power grids at the mercy of Russian hackers, and the menacing build-up of nuclear and other arms – of which increased European military spending is a part – produce an image of advanced preparations for war on a scale that would necessitate global social mobilization to prevent it, of the type organized and analyzed by the left more than a generation ago.[185]

At the same time, the global political-economic and diplomatic framework in which these developments take place is quite distinct from that of the Cold War. For one, neo-liberalism, however much its reputation may have been battered by successive economic crises, retains global paramountcy.[186] No other legitimating principle of capitalism has developed yet to rival it, and neither has any trenchant anti-systemic opposition been able to dislodge it from below. Secondly, the largest powers and presumed belligerents in this new face-off – the US, Russia and China – are either more dramatically unequally matched in military affairs than they were 70 years ago (US-Russia); or additionally they are essentially interdependent (US-China) in the context of a far more fragile regime of global capital accumulation than that which existed at any time during the height of the Cold War in the early 1960s, or even during its second iteration in the 1980s. Russia, after a decade of catastrophic liberalization under US tutelage, has over the more recent period stabilized its economy at a nominal GDP roughly equivalent to that of Brazil, though it is well behind Canada and Italy (Russian GDP is a twentieth of the US's). China and the US are each other's largest trading partners, and the former has for two decades subsidized its own exports to US consumers by underwriting US debt, binding the two societies ever closer together.

Still, the overall frailty of this global regime has inflamed at least two further internal stresses on it. One is the growing inability of nearly all societies currently to reproduce an adequate measure of employment and living standards for large segments of their populations – as can be seen in the rustbelts of both China and the US, the hinterlands of Europe and even in the downward mobility of educated urban populations.[187] The unpredictable political consequence of this dynamic means each respective state in question has had to contend with significant erosion of its claim to legitimacy and eruptions of "populist" or other discontent. Second, for the same reasons of flagging economic performance, capital is increasingly dependent on the state: where profitable investment in production is more difficult, redistribution upward through corruption has established itself.[188] Sectors of capital closest to the state – aside from finance, those which orbit the military, police and intelligence services – stand to benefit economically, but they also may rightly anticipate that repression will play an increasingly important role in managing society.

National politicians who face mounting pressure to restore or improve standards of living, but cannot without undermining the decrepit international order which sustains them; a hypertrophy of the repressive arm of the state and those profiteering from it: these factors combined mean that international tension will blend into domestic politics. In the US, on top of this, as has been discussed, sits a layer of imperial strategists who have been committed since the 1990s to the restraint and management of China and of the integration of Russia into its sphere of influence. This does not necessarily take the form of outright war, but it entails that those independent uncooperative paths of development for Russia and China – conceivably forced by the economic realities

185 See Lucio Magri, "The Peace Movement and Europe," in *Exterminism and Cold War* (London: New Left Books, 1982), pp. 126, 132.
186 For the definitive study in English of neo-liberalism's international origins and development, see Philip Mirowski and Dieter Plehwe (eds.), *The Road from Mont Pèlerin* (Cambridge: Harvard University Press, 2009).
187 For more on the Chinese rustbelt, see Ching Kwan Lee, *Against the Law: Labor Unrest in China's Rustbelt and Sunbelt* (Berkeley and Los Angeles: University of California Press, 2007), pp. 120-27 and 140-53.
188 This dynamic has been anatomized by the US historian Robert Brenner.

putting all societies under pressure concurrently – would be a source of increasing friction. Under such conditions, it is entirely plausible that a previously symbiotic arrangement among the major states, even with its occasional disruptions, would develop into one of open and sustained antagonism.

Against this geopolitical backdrop, the primacy of shaping public opinion takes on even greater significance, as it is overdetermined by both domestic and international pressures. This is especially the case in Europe, whose consolidation as an Atlanticist stronghold has long been understood as a prerequisite for containment of Russia and China, and where economic incentives are for its large companies no less enticing than elsewhere. One component of the management of public opinion in this vein has been the use of Europe's NATO think tanks, which are closely tied to the US state and private interests. As political parties or associations are transformed into administrative rather than mass-membership organizations,[189] these centers of expertise take on new importance. Because think tanks develop compact causal explanations of critical events and social life, they are now essential in the domains of international relations and security. There, the distinction between friend and enemy can depend on the explanation given regarding foreign threats – whatever its merit, and however impoverished the evidence amassed or manufactured. To compensate, think tanks often market themselves as trusted centers of expertise and wear the conventional signs of academic respectability.

As the case studies in this report have demonstrated, NATO advances its interests in Europe by way of specific methods for the management of public opinion. These count on the formulation of certain frameworks, or "narratives," as outlined by Stratcom and GLOBSEC's agenda for collaboration with film studios and publishers. Intensified use of "memetic," psychological and information warfare, also boosted by Stratcom, must be read in the context of those exercises in digital sabotage undertaken by the Cooperative Cyber Defence Centre.

These latter methods indicate that in addition to shaping a narrative framework suitable to its aims, NATO's public relations are also designed to work on the more fundamental register of perception itself. This aspect of public opinion was already identified in 1922 by US journalist Walter Lippmann, who saw in the use of the image, and in the altered time and attention of the mediatized public sphere, the importance of unconscious association.[190] Edward Snowden's revelations in 2013 showed that British intelligence concerned itself with the active manipulation of perception online by various means, including simulation ("showing the false") to camouflage rather than strictly conceal outright its own activities, among which included misdirection and repetition to generate specific expectations.[191] It can only be assumed that the systematic repetition of accusations against a supposed foreign enemy fits this model.

The mounting contradictions of the world economy have raised the stakes for the US empire and its NATO auxiliaries. The 2003 US attack on Iraq indicated just what type of extreme measures these institutions will take – in war itself and in the preparatory falsifications used to justify it. As the self-critique undertaken by NATO's communications department indicates, the alliance is capable of learning from its errors. All progressive forces in society should be prepared to do the same.

189 For further discussion of this in its European context, see Peter Mair, *Ruling the Void: The Hollowing of Western Democracy* (New York and London: Verso, 2013), especially pp. 93-98.
190 See Walter Lippmann, *Public Opinion* (New York: Macmillan, 1922), pp. 15, 31, 58-63.
191 These are all outlined in the classified GCHQ tutorial for online manipulation, leaked by Snowden in 2013 and published a year later. See page 16 (footnote 43), above.

The Left in the European Parliament
Rue Wiertz 43 B-1047 Brussels
www.left.eu