EUISS
EUROPEAN UNION
Institute for Security Studies

CONFLICTS TO COME

15 scenarios for 2030

Edited by
Florence Gaub

With contributions from
Natasha E. Bajema, Lotje Boswinkel, Daniel Fiott, Franz-Stefan Gady, Zoe Stanley-Lockman, Kathleen J. McInnis, Nicolas Minvielle, Andrew Monaghan, Katariina Mustasilta, Ali Fathollah-Nejad, Patryk Pawlak, Tobias Pietz, Sinikukka Saari, Stanislav Secrieru, Simona R. Soare, Bruno Tertrais and Olivier Wathelet

CHAILLOT PAPER / 161
December 2020

European Union Institute for Security Studies (EUISS)

100, avenue de Suffren
75015 Paris

http://www.iss.europa.eu
Director: Gustav Lindstrom

print		online	
	ISBN 978-92-9198-973-7		ISBN 978-92-9198-972-0
	CATALOGUE NUMBER QN-AA-20-005-EN-C		CATALOGUE NUMBER QN-AA-20-005-EN-N
	ISSN 1017-7566		ISSN 1683-4917
	DOI 10.2815/101723		DOI 10.2815/966219

Published by the EU Institute for Security Studies and printed in Belgium by Bietlot.
Luxembourg: Publications Office of the European Union, 2020.
Cover image credit: Daniel Cheung/unsplash

EUROPEAN UNION
Institute for Security Studies

CONFLICTS TO COME

15 scenarios for 2030

Edited by
Florence Gaub

With contributions from
Natasha E. Bajema, Lotje Boswinkel, Daniel Fiott, Franz-Stefan Gady, Zoe Stanley-Lockman, Kathleen J. McInnis, Nicolas Minvielle, Andrew Monaghan, Katariina Mustasilta, Ali Fathollah-Nejad, Patryk Pawlak, Tobias Pietz, Sinikukka Saari, Stanislav Secrieru, Simona R. Soare, Bruno Tertrais and Olivier Wathelet

CHAILLOT PAPER / 161
December 2020

The editor

Florence Gaub is the Deputy Director of the EUISS. She specialises in strategic foresight, as well as security and conflict in the Middle East and North Africa.

The EUISS Chaillot Paper series

The *Chaillot Paper* series, launched in 1991, takes its name from the Chaillot hill in the Trocadéro area of Paris, where the Institute's first premises were located in the building occupied by the Western European Union (WEU). The hill is particularly known for the Palais de Chaillot which was the site of the signing of the UN Universal Declaration of Human Rights in 1948, and housed NATO's provisional headquarters from 1952 until 1959.

CONTENTS

ON THE FUTURE OF CONFLICT

by
FLORENCE GAUB

There is a rule of thumb in foresight: the larger the human factor in the field whose future you are trying to anticipate, the more difficult it will be to get it right. The reason is simple: ourselves. No other future factor is as stubborn to predict, or as hard to understand as the human being. Quite in contrast to the bold claims of rational choice theory, human behaviour is not easily modelled, whether at personal or state level. Nowhere does this become more apparent than in the diverse and contradictory body of knowledge seeking to understand why conflicts among humans emerge, continue or end, and how they are being fought. As one study put it, "history is littered with mistaken predictions about the future of warfare".[1]

Because conflict is deeply existential, destroying lives and livelihoods, it is also a phenomenon that many researchers have tried to understand better in order to make it more predictable – and, indeed, they should continue to do so. After all, despite claims that conflict will soon disappear altogether, it is still very much present today – and the last decade in particular has seen an increase in the number of violent conflicts around the world.[2] Since 2010, nearly 900,000 lives were lost to politically motivated violence, and in 2019 alone the world witnessed 121 active conflicts.

There have been broadly three approaches used to anticipate conflict: those looking at push-factors (including aspects such as socio-economic development, political institutions and arms acquisitions), those looking at pull-factors (including the regional or international context), and those trying to understand the shape and tactics of conflicts to come. Whereas the insights of the first two are primarily useful to policymakers interested in conflict prevention, the latter is useful to those preparing for the worst-case scenario, war.

The first area, looking primarily at internal causes for conflict, has made remarkable progress over the last decade thanks to Big Data and Artificial Intelligence (AI). Models such as the Early Warning Project or Uppsala University's ViEWS, Lockheed Martin's Integrated Crisis Early Warning System, or the EU's Conflict Early Warning System (CEWS) use historical data on conflicts and their (assumed) drivers and statistical inferences and machine learning techniques to forecast future conflict trends.[3] Working within a window of 1-36 months before conflict onset, their predictive accuracy can reach 80% – but they are better at forecasting the continuation of a conflict or spill-over of conflicts than anticipating new conflicts.

1 Raphael S. Cohen et al., *The Future of Warfare in 2030: Project Overview and Conclusions* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR2849z1.html.

2 Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Penguin, 2011); Aaron Clauset, "Trends and fluctuations in the severity of interstate wars", *Science Advances*, February 2018, https://advances.sciencemag.org/lens/advances/4/2/eaao3580#toc.

3 Tate Ryan Mosley, "We are finally getting better at predicting organized conflict", *MIT Technology Review*, October 24, 2019, https://www.technologyreview.com/2019/10/24/238426/predicting-organized-conflict-ensemble-modeling-ethiopia-ahmed/; Matina Halkia et al, "The Global Conflict Risk Index: Artificial Intelligence for Conflict Prevention", JRC Technical Reports, 2020, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118746/ai_gcri_technical_report.pdf.

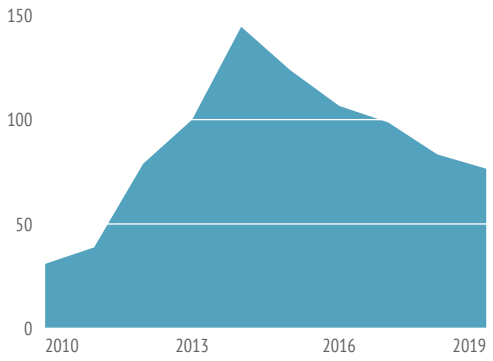
But for the time being, they are only of limited use to policymakers. One of the reasons is that they focus on conflict probability, but not on conflict pathways. Rather than measure *how* a conflict unfolds, these models measure *under what conditions* it is likely to erupt. For policymakers wishing to prevent a conflict, this is of limited use: they will need to know exactly where the pressure needs to be relieved in the instant, a qualitative question these models cannot answer.[4] In addition, these models cannot offer insights into how the conflict will be fought. This is important to know because it could indicate the lethality of the conflict and the impact on the economy and people's livelihoods. Lastly, these models mainly aim at forecasting armed violence *within* a state, rather than *between* states. Even though the latter might be less frequent today, it is still of importance for decision-makers. Perhaps most importantly, these models cannot incorporate novelty: because they are based on data relating to past conflicts, they have no room for hitherto unknown drivers of conflict.

In sum, these models are not yet ready to serve as a basis for decision-making – here, old-fashioned qualitative analysis on drivers and possible solutions will be the safer bet for the time being.[5]

The second approach, largely established during the Cold War, posits that conflict likelihood depends on the international or regional system of which a state is part. Born out of inductive thinking rather than data, international relations theory was, in effect, an attempt to "understand international politics, grasp the meaning of contemporary events, and foresee and influence the future", as the founder of the discipline, Hans Morgenthau, stated.[6] His main assumption was that the international state system was anarchic, and as a result insecure. Because states can never be sure about the behaviour of other states, they are in a 'security dilemma': no war is certainly the best option, but it is not the most certain one.[7] When applied in *hindsight*, this theory seemed to explain a host of conflicts such as World War I, the origins and end of the Cold War, and conflicts in Yugoslavia and Africa.[8]

Conflict-related deaths

2010–2019, thousand



Data: Uppsala Conflict Data Programme, 2020

But in this theoretical field, too, prediction quality was low and, worse, policy recommendations few and far between. Neither the often-repeated dictum that bipolarity makes for more stability could be proven, nor the opposite stating that unipolarity would achieve this.[9]

4 Guo Weisi et al., "Retool AI to forecast and limit wars", *Nature*, October 15, 2018, https://www.nature.com/articles/d41586-018-07026-4#ref-CR1.

5 Lars-Erik Cederman and Nils B. Weidmann, "Predicting armed conflict: Time to adjust our expectations?", *Science*, February 33, 2017, https://science.sciencemag.org/content/355/6324/474; Thomas S. Szayna et al., "Conflict Trends and Conflict Drivers: An Empirical Assessment of Historical Conflict Patterns and Future Conflict Projections" (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1063.html.

6 Hans Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (New York: Knopf, 1948), pp. 4-5.

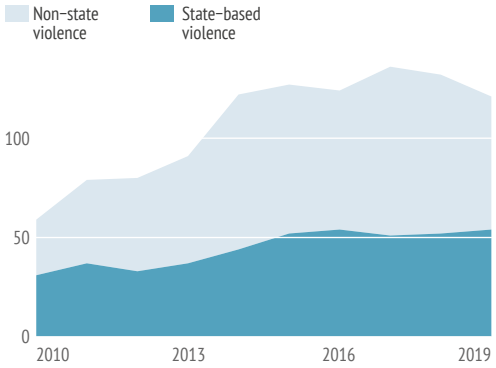
7 John Stoessinger, *Why Nations Go to War* (New York: St. Martin's Press, 1997); Geoffrey Blainey, *The Causes of War* (New York: Free Press, 1988); Kori Schake, "What Causes War?", *Orbis*, vol.61, no. 4, 2017, pp. 449-62.

8 Barry Posen, "The Security Dilemma and Ethnic Conflict", *Survival*, vol. 35, no. 1 (Spring 1993): pp.27–47; Robert Jervis, "Was the Cold War a Security Dilemma?" *Journal of Cold War Studies*, vol. 3, no. 1 (Winter 2001): pp. 36–60.

9 Michael D. Wallance, "Alliance Polarisation, Cross-Cutting and International War, 1815 – 1964: A Measurement Procedure and Some Preliminary Evidence" in J. David Singer (ed.), *Explaining War: Selected Papers from the Correlates of War Project* (Beverly Hills : Sage Publications, 1979), p.105; Michael C. Webb and Stephen D. Krasner, "Hegemonic Stability Theory: An Empirical Assessment", *Review of International Studies*, Special Issue on the Balance of Power,vol. 15, no. 2 (April, 1989): pp. 183-98.

Conflicts

Total number per year and conflict type, 2010-2019



Data: Uppsala Conflict Data Programme, 2020

Perhaps crucially, these theories remained silent on internal conflict which is the dominant form of conflict in the twenty-first century.

The arrival of data in the field raised hopes of new insights into the conditions under which war and peace emerged: projects such as the Correlates of War promised "theory-based prediction".[10] But the outcome was below expectation, producing "neither theory, nor forecasts, nor useable policy recommendations."[11] In large part, this had to do with the fact that international relations is not a data-heavy field. There are no numbers on concepts such as 'polarity', 'deterrence' or 'hostility', and it is near to impossible to survey the perceptions and decision-making processes leading to conflict – the little that there is is mostly reconstructed *post-factum*, including an often falsifying hindsight bias. Indeed, because conflict is overall a rather rare event, we generally have only limited data to develop a comprehensive picture of its onset, evolution and ending.[12] Data scarcity has not stopped some from calculating the likelihood of a nuclear war: the doomsday clock, which symbolically displays the proximity to 'midnight' (which stands for war) has been continuously reminding policymakers and publics alike of the horrifying possibility of nuclear conflict. At the opposite end of the scale are those adhering to deterrence theory: the idea that the possession of nuclear weapons alone suffices to prevent war.[13] A distant cousin to this field is cliodynamics, a field searching for patterns in human history. Followers of this school are persuaded that complex human societies are affected by recurrent and therefore predictable waves of conflict.[14] The field is heavily criticised for perceiving human life as a constant repetition regardless of culture, location or point in time – but perhaps worse, it fails to offer ideas on what to do with the knowledge that a conflict is imminent. Most importantly, this approach, like the others mentioned, is incapable of incorporating novelty as it is entirely built on the past – an approach inherently flawed as no two conflicts are ever alike.

The third approach to conflict focuses on the ways and means with which conflicts will be fought. As a result, it has no ambition to develop generalised theories, or predict a conflict's onset before it actually happens. Instead, its contribution is to ready societies and institutions for a coming conflict. Whereas the first two schools use either history or assumptions about the world as starting points for conflict anticipation, this approach combines the two with imagination. It is therefore the only field that can incorporate hitherto unknown elements of conflict, be it technological innovation, environmental changes, or ideologies yet to be born. Because of this, and because concrete policy ideas can be deducted from it, of the three it is the one of the greatest use for policymakers – when they decide to act on the findings. Before the invasion of Iraq, it was works

10 Quoted in John Lewis Gaddis, "International Relations Theory and the End of the Cold War", *International Security*, vol. 17, no. 3 (Winter, 1992-1993), pp. 5-58.

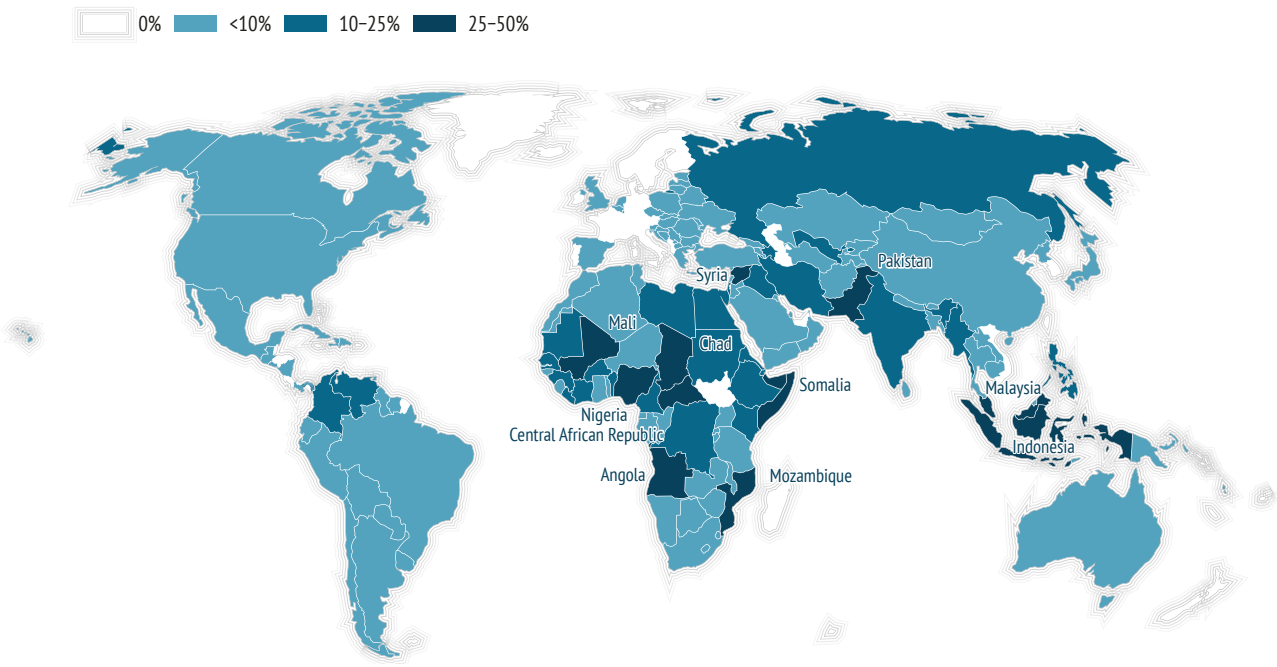
11 Ibid.

12 Thomas Chadefaux, "Conflict forecasting and its limits", *Data Science*, no.1, 2017.

13 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1967).

14 Peter Turchin, "Political instability may be a contributor in the coming decade", *Nature*, vol. 463, February 3, 2010, https://www.nature.com/articles/463608a.

Probability of experiencing a new conflict
In the years 2019-2024



Data: Cherikou and Hanouti, 2020

from this field that accurately anticipated the chaos in Baghdad as well as regional instability. Unfortunately, these warnings were not followed up by necessary precautions.[15]

Using imagination to anticipate the long-term future emerged in Europe at a time of steep technological progress at the end of the nineteenth century. Literature by Jules Verne and H.G. Wells, among others, attempted to digest the impact technology would have on human societies. But it was conflicts such as the Franco-Prussian war and World War I that spurred on developments in this field because neither unfolded in the expected way. Anticipation hence became a tool to reduce surprise. In contrast to the other two approaches which rely on science, history, and deduction (asking "what is?") this field adds imagination, novelty, and art (asking "what if?") to paint a detailed picture of conflicts to come.

To be clear: this field, too, suffers from the same degrees of inaccuracy as the other two. Where this is the case, it derives primarily from being tied to advocacy – the desire to trigger a policy change; to the present – seeing the future as an extrapolation of today's trends; or from disruptive illusion – the idea that future conflicts will be completely different from past ones.[16]

But it has its merits. Stories on the future of conflict expose our assumptions, our fears, and what we think can be done to assuage them. They offer insights into what we think will trigger a dispute, the conflict parties we consider relevant, and the assessment we make of our existing capabilities. Perhaps most

15 James Fallows, "Blind Into Baghdad," *Atlantic Monthly*, January/February 2004; Eric Schmitt and Joel Brinkley, "State Department Study Foresaw Trouble Now Plaguing Iraq," *New York Times*, October 19, 2003; "War Games In '99 Predicted Iraq Problems", *CBC News*, November 4, 2006, https://www.cbc.ca/amp/1.597956.

16 H. R. McMaster, "Discussing the Continuities of War and the Future of Warfare", *Small Wars Journal*, October 14, 2014, https://smallwarsjournal.com/jrnl/art/discussing-the-continuities-of-war-and-the-future-of-warfare-the-defense-entrepreneurs-foru.

importantly, scenarios and fiction invite a reflection that pure analysis cannot. As one of the contributors to this volume puts it, "knowledge without imagination can tell you where you are but not where to go."[17] It is perhaps for this reason that fictional accounts had and continue to have more of an impact on policymakers than academia.[18] A series of novels, such as *The Battle of Dorking* (1871), or *The Great War in England in 1897* (1894) imagined the invasion of Great Britain by various actors. Since then, 'FICINT' (Fictional Intelligence), "a deliberate fusion of narrative's power with real-world research's utility" has carved out an important niche in the works on the future of conflict.[19]

Despite their limited predictive capability, books such as *War with Russia* (2017) or *The 2020 Commission Report on the North Korean Nuclear Attacks against the United States* (2018) all heavily influenced how strategic communities around the world reflected on future conflict. In part, this is because the emotion stories can generate allows for a greater degree of influence and even reflection. Novels such as *From Russia with Love*, *Red Storm Rising* and more recently *Ghost Fleet* but also films such as *WarGames* all shaped the perception of the future of conflict of John F. Kennedy, Ronald Reagan and NATO's Admiral James Stavridis.[20] Not just fiction can be included in this field, but also speculative analysis on what the next conflict might look like. Works like *Is War Now Impossible?* (1898) or H.G. Wells' *War in the Twentieth Century* (1902), but also recent ones like *Wired for War* (2011) or *The Drone Age* (2020), extrapolate from technological innovation to understand what future conflict could look like.[21] War-games and scenarios, too, can be included in this field, as they rely not just on the past, but also the future to put together an approximate idea of what conflict could look like.[22]

This *Chaillot Paper* belongs to the third school of conflict anticipation in that it uses imagination along with past and present trends. Crucially, it is not limited to the means and ways of conflict. It is precisely for this reason that we prefer the term 'conflict' over 'war': it is to highlight our interest in all aspects of a conflict, including the causes and long-term effects. This way, we hope to contribute to both clusters of policymakers thinking about the future of conflict: those seeking to prevent it, and those seeking to manage it.

A word on methodology. The authors in this volume were given no further instruction other than to imagine a conflict set in 2030. (The year 2030 should, however, not be taken literally: as in the visual arts, we use the date to create a future perspective for both authors and readers rather than to set a firm deadline.) The chapters were arranged only afterwards into categories that emerged from the collective body of contributions. They were asked explicitly to avoid as far as possible trends extrapolation, and to look for weak signals, or elements of conflict that are not (yet) in the headlines. They were not allowed to be too fantastical: no aliens, fictional countries, or non-existing technology were to be used. After all, this work is not science fiction, but fictional intelligence (FICINT): rooted in reality.

But because the scenarios present situations that are unexpected or surprising, they are probably not perceived as very likely – but this

17 Kathleen McInnis, "Strategists have forgotten the power of stories", *Foreign Policy*, May 19, 2020, https://foreignpolicy.com/2020/05/19/national-security-policymaking-mythos-logos-strategy/

18 J Furman Daniel and Paul Musgrave, "Synthetic Experiences: How Popular Culture Matters for Images of International Relations", *International Studies Quarterly*, vol. 61, no.3, September 2017, pp. 503–16.

19 August Cole and P.W. Singer, "Thinking The Unthinkable With Useful Fiction", *Journal of Future Conflict*, Online Journal, Issue no. 2 (Fall 2020): CD&E, doctrine and lesson learned in support of future interstate conflict.

20 Franz-Stefan Gady, "The Impact of Fiction on the Future of War", *The Diplomat*, December 7, 2019, https://thediplomat.com/2019/12/the-impact-of-fiction-on-the-future-of-war/; Fred Kaplan, "'WarGames' and Cybersecurity's Debt to a Hollywood Hack", *The New York Times*, February 19, 2016, https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html.

21 Lawrence Freedman, *The Future of War: A History* (London: Allen Lane, 2017), pp. 61-70.

22 Paul Cornish and Kingsley Donaldson (eds.), *2020: World of War* (London: Hodder & Stoughton, 2018).

should serve even more as a reason to engage with them. After all, most conflicts come as a surprise (but seem entirely predictable in retrospect).

The group of authors were chosen mainly for their subject matter expertise, but as a collective they are far from being homogenous. This is a conscious choice to avoid groupthink, perhaps the greatest danger in foresight.[23] But of course, the careful reader will understand that they are not offering a comprehensive picture of the future of conflict: instead, it is a collective reflection on what we believe conflicts to come could look like – and what that would mean. The scenarios thereby contribute to, and at times challenge, the existing body of assumptions when it comes to conflict, its likelihood and trends likely to influence upcoming conflicts. Here, a surprising consensus emerges from speculative analysis – but instead of indicating certainty, it could also simply indicate a collective bias.

After all, most conflicts come as a surprise (but seem entirely predictable in retrospect).

> Conflicts are assumed to be more common in the future. This expectation derives from a number of assumptions: geopolitical tensions, the rise of civil activism, slow economic growth and the effects of climate change on weak states all feature in the perception that the likelihood of all types of conflict will increase – including direct confrontation between major powers.[24] To be sure, this assumption does not rest on an ongoing trend as conflicts have declined continuously since the end of World War II.

> Conflicts are assumed to be both more and less violent. Lower lethality is expected on the one hand because hybrid methods do not cause large-scale casualties – in turn, this could also make conflicts more frequent as preventing and resolving them is harder.[25] This assumption is an extension of the trend of casualty decline over the last decades. On the other hand, casualties could also rise because conflicts are assumed to take place amid civilian life, be it in cities or in cyberspace.[26] A third option could be that although total numbers of casualties decrease, public opinion could continue to veer towards ever lower levels of tolerance in this regard.

> Conflicts are expected to last longer. This is another extrapolation of a trend visible for over two decades: in 2020, 60% of active armed conflicts around the world have been going on for at least 10 years – but there is no solid evidence for the reason.[27]

> Battlefields will be urban: where urbanisation, climate migration, and digitalisation merge, future conflicts must take place in cities – or so the reasoning goes.[28] But because spatial conflict theory is still in its infancy, this assumption does not rest on solid evidence.[29] Indeed, it is challenged by the fact that past and present conflicts, too, have an

23 Elna Schirrmeister et al., "Psychological biases and heuristics in the context of foresight and scenario processes", *Futures and Foresight Science*, February 2020, https://onlinelibrary.wiley.com/doi/10.1002/ffo2.31.

24 Op. Cit., *The Future of Warfare in 2030: Project Overview and Conclusions*, p.53; National Intelligence Council, *Global Trends: Paradox of Progress*, January 2017, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf.

25 Sarah Bressan and Mari-Liis Sulg, "Welcome to the grey zone: future war and peace", *New Perspectives* , vol. 28, no.3, 2020, pp. 379-97, https://journals.sagepub.com/doi/pdf/10.1177/2336825X20935244.

26 Darran Anderson, "The grim future of urban warfare", *The Atlantic*, December 11, 2018, https://www.theatlantic.com/technology/archive/2018/12/technology-will-make-war-even-worse/577723/

27 The International Institute for Strategic Studies, *Armed Conflict Survey 2020*, https://www.iiss.org/press/2020/acs-2020.

28 Modern War Institute, Urban Warfare Project, John Spencer and David Kilcullen, "Out of the mountains, revisited", podcast, December 7, 2019, https://mwi.usma.edu/announcing-urban-warfare-project-podcast/

29 Annika Björkdahl and Susanne Buckley-Zistel, *Spatializing Peace: Mapping the Production of Places, Sites and Scales of Violence* (New York: Palgrave MacMillan, 2016).

overwhelming tendency to be urban, whether in Iraq, Syria, Libya, Belarus or Ukraine.

> Technology will affect the battlespace: innovations such as AI and robotics will change the way conflict is conducted – but it is not clear whether AI applications such as drone swarms and software vulnerability discovery tools will give an advantage to offensive or defensive military operations.[30] If AI favours offence, it could indeed make conflict an interesting option for some – but if it favours defence, it would make conflict less likely. The problem with anticipating either is that new forms of force require new tactics which normally emerge from trial and error.[31] If history is an indication, it will not alter the field as decisively as anticipated (in fact, most past predictions go wrong when they overestimate the technological factor – and underestimate the human one). [32] That said, the mere idea of AI potentially giving an advantage to an aggressor will lead to investments and therefore ubiquity. [33]

> Actors are assumed to be diverse. As emerging autonomous and gamified technologies and cyberwarfare tactics become cheaper and thus more accessible, the threshold for warfare by non-state actors is lowering. As a result, future conflicts are expected to involve growing numbers of guerrilla groups, hackers, terrorists, private security companies, and other types of irregular actors. Yet even though the number and diversity of conflict actors will increase, states will remain the central actors in future conflicts – this, too, is an extrapolation of an ongoing trend. [34]

How to read the scenarios

The contribution of this *Chaillot Paper* is to engage, invite to a reflection on readiness, conflict and resources rather than to make concrete predictions. The advantage for the reader will be that once conflict comes, he or she will be more prepared – the neural pathways will have a faster response ready due to the fact that the scenarios presented will have stimulated the reader's imagination.[35] When reading the scenarios, it might be useful to keep the following considerations in mind:

> Challenge the assumptions preceding each scenario, and determine under which conditions they are invalidated;

> Formulate your own assumptions and under which conditions they would have to change;

> Imagine the political and military implications of these scenarios for Europe;

> Think through various ways in which the scenarios could unfold differently.

Warm thanks go, as always, to all those who made this publication come about: Gustav Lindstrom, the director of the EU Institute for Security Studies without whose continuous support innovative thinking would not be possible; Gearóid Cronin for his thorough editing; Christian Dietrich for making ideas visually appealing; and Lotje Boswinkel for her hard work and dedication. Lastly, gratitude goes to all the authors who decided to embark on a truly innovative project taking them out of their comfort zone and into the realm of foresight.

30 Daniel Fiott and Gustav Lindstrom, "Artificial Intelligence: What implications for EU security and defence?", EUISS *Brief* no. 10, November 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2010%20AI.pdf.

31 Ben Garfinkel and Allan Dafoe, "Artificial Intelligence, foresight, and the offense-defense balance", *War on the Rocks*, December 19, 2019, https://warontherocks.com/2019/12/artificial-intelligence-foresight-and-the-offense-defense-balance/

32 Michael E. O'Hanlon, "A retrospective on the so-called revolution in military affairs, 2000-2020", Brookings, September 2018, https://www.brookings.edu/research/a-retrospective-on-the-so-called-revolution-in-military-affairs-2000-2020/

33 Peter L. Hickman, "The future of warfare will continue to be human", *War on the Rocks*, May 12, 2020, https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/

34 Sean McFate, "The Return of Mercenaries, Non-State Conflict, and More Predictions for the Future of Warfare", *Medium*, February 22, 2019, https://gen.medium.com/the-return-of-mercenaries-non-state-conflict-and-more-predictions-for-the-future-of-warfare-7449241a04e5.

35 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Penguin, 2012).

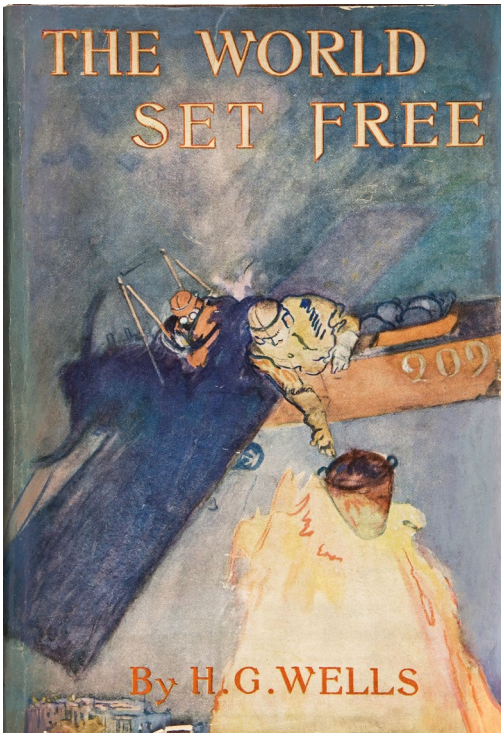
ON THE USE OF SCIENCE FICTION FOR CONFLICT FORESIGHT

by
NICOLAS MINVIELLE AND OLIVIER WATHELET

Imagination plays a guiding role when it comes to the future. Not because it predicts it – science fiction writers are trying hard to counter this widespread misapprehension – but because by dreaming up future scenarios, it questions, tests and creates plausible worlds. Studying the various ways in which imagined notions of the future and the actual reality of the future meet – and sometimes fail to correspond – improves our ability to project, and be prepared. Imagining the future also influences how the future will play out: ideas circulate between creative industries and economics, politics and social fields, leading to cross fertilisation and joint development. This can range from products inspired by set elements, interaction sequences or prototypes developed for novels, films or comic books. From the digital tablet (inspired by *Star Trek*) to the geostationary satellite programme (first formulated by the novelist Arthur C. Clarke), there are many examples of products or strategies that have been tested and described for the first time in a work of fiction. An idea of the future is passed around the many different actors that make it, and then is taken up by the general public. Designers extend some of its principles. And so on and so forth. The term 'loop-looping' is used to designate these back and forth trips between worlds that contribute to making the 'imagining' of ideas a stage in a process of innovation to be thought of on a collective scale.

The military field is no exception to this rule. The atomic bomb and its use, for instance, was first imagined by H.G. Wells in 1914, in his novel *The World Set Free*. He described a bomb dropped from an aircraft in a (then) hypothetical conflict between Britain, France, America

The World Set Free
Cover of the first edition, 1914



and Germany and Austria. Of course, Wells did not 'invent' the concept, but rather fleshed out somebody else's idea – that of a scientist, Frederick Soddy, himself a pupil of the physicist Ernest Rutherford. Soddy, unlike his teacher, believed in the possibility of controlling atomic energy. It was a marginal idea at the time, but one that Wells used to construct his story and invent the principle of a nuclear weapon. Wells' story went on to influence Hungary's Leo Szilard, who invented the chain reaction in 1934. The principle of the nuclear bomb was now made not only possible but plausible. Thus, science fiction does not predict conflicts, but tests ideas of conflict in tandem with those that play an active role in setting the scientific agenda.

Works of fiction therefore have the potential to test and transform ideas and concepts, contributing not only to their dissemination but also to their enhancement in terms of relevance and plausibility.

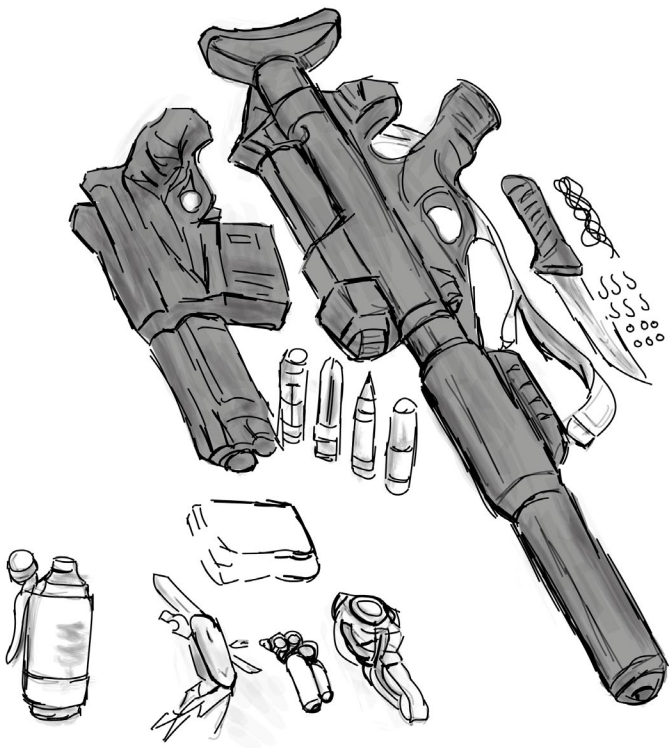
This process can be stimulated by two approaches. The first is to increase the contribution of authors and creators from around the world when it comes to conceptualisations of the future. One such example is the Red Team approach currently underway within the French armed forces. The second is to leverage existing creative works. For instance, the French FELIN (*Fantassin à Équipement et Liaisons Intégrés – Integrated Infantryman Equipment and Communications*, an infantry combat system) has a firing capability directly inspired by the 1980s Japanese manga *Apple Seed* (1985-1988).

Popularised technologies ...

Creativity and innovation are not necessarily what we think. For most of us, innovative, original ideas appear to be simply 'born' out of nowhere. But in reality, innovation is an aggregative process whereby existing ideas are put together in a new way. Rather than looking for 'nuggets' within works of fiction (i.e. the one idea that gets the future right) it is more useful to look at the process of 'mundanisation',[1] i.e. the process where innovation jumps from the page and catalyses an (often) technological, but also social, or more rarely, political, rupture.

This applies to the military, too. Although war is a state prerogative, this has not stopped creative works (particularly manga) from imagining how warfare might evolve in the future and thereby directly influencing it. Drones are just one example. For instance, in *Ghost in The Shell* (1989-1991), regalian forces are regularly confronted with sophisticated military-level equipment and techniques (exoskeletons, cyberattacks, etc.) from non-state groups. In one episode, the heroine thus finds herself tracking a submarine with capabilities currently unavailable to the armed forces. The suspension of disbelief induced by the manga allows us to accept this technological breakthrough and to wonder about the plausible consequences. What would really happen if, for example, migrant smugglers or mafias were able to have equivalent submarines?

Manga weapons
Apple Seed, 1980s



1 This refers to the process of projecting elements of a fantasy world into a real-life setting. See: https://tvtropes.org/pmwiki/pmwiki.php/Main/Mundanization.

What happens when civilian exoskeletons become as powerful, or even more powerful, than those of the military? When human augmentation becomes accessible to anyone with a 3D DNA printer? When encrypted quantum satellite networks become accessible to anyone? This raises the question of the cascade in military technology: the unbridled search for technological superiority has an immense financial cost but offers *de facto* future capabilities at lower cost to potential enemies.

... and extreme technologies

If the imagination offers us visions of futures where technology is popularised, it also allows us to discover futures where technology is used in an extreme way in conflicts. A certain number of themes are recurrent. The enhancement of the human being is certainly one of the recurring tropes, whether mechanically with the use of *Iron Man*-type armour, especially in manga, or biologically with the recurring serums of the super soldier (see *Captain America*). The manga *Terra Formars* (2011) presents a humanity that can appropriate animal genes through the 'Mosaic Organ Operation': the strength of the spider, the hornet's sting etc are on offer for anyone who can survive the operation. The result is striking in the diversity of conflicts offered: what is a shark man worth compared to a bee man?

Humans in insectoid form
Terra Formars, 2001

Man-machine collaborations are eminently numerous and often well narrated. The flying drone depicted in the science fiction film *Stealth* (2005), for instance, offered a future vision of the flying buddies on which all military forces are currently working, while robotic mules are presented as essential assistants in many works (e.g. Marguerite in the graphic novel *Soleil Froid*).

Finally, the classic vision of the networked man offered by cyberpunk authors, working in close partnership with AI, or becoming himself a digital form, is more and more prevalent. This offers radical visions of men wearing and controlling extremely complex armours of all sorts able to carry out many operations at once: attacking in cyberspace coupled with

Combat exoskeleton
Elysium, 2013
(science fiction film directed by Neill Blomkamp)

a physical assault at the same time. In this vein, the Franco-Belgian comic book series *Travis* offers some interesting examples.

Imagined futures that show the limits of current designs

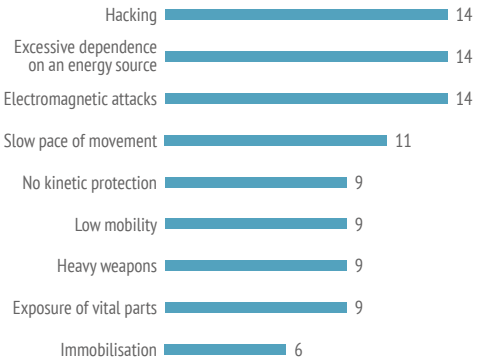
When fiction writers speculate about future conflicts, they also allow actors to respond and adapt to often more powerful enemy technologies. In that sense, fantasy tends to test the limits of techno-centric approaches. The heroine of *Apple Seed*, for instance, overpowers an imposing cyborg with simple laser jamming. Extreme technologies break down because of the sand in the *Marvel* universe. *Iron Man* armour is shattered by axes attacking the joints in *Chaos Team*.

Works of fiction and graphic novels imagining future warfare scenarios therefore stress also the extreme dependence of new technologies on their environment. In addition, they speculate on possible new problems. In the world of Carmen McCallum (the eponymous heroine of a French comic book series by Fred Duval), the armed forces have very advanced drones and equipment that can be almost systematically defeated by a human being ... with little or no increase in technological skills. This aspect deserves to be integrated into the training of infantrymen.

Warrior clad in exo-armour
Travis, 2002

Travis, vol. 5, "Cybernation"

Common military weaknesses in fiction
In a corpus of 289 fictional works



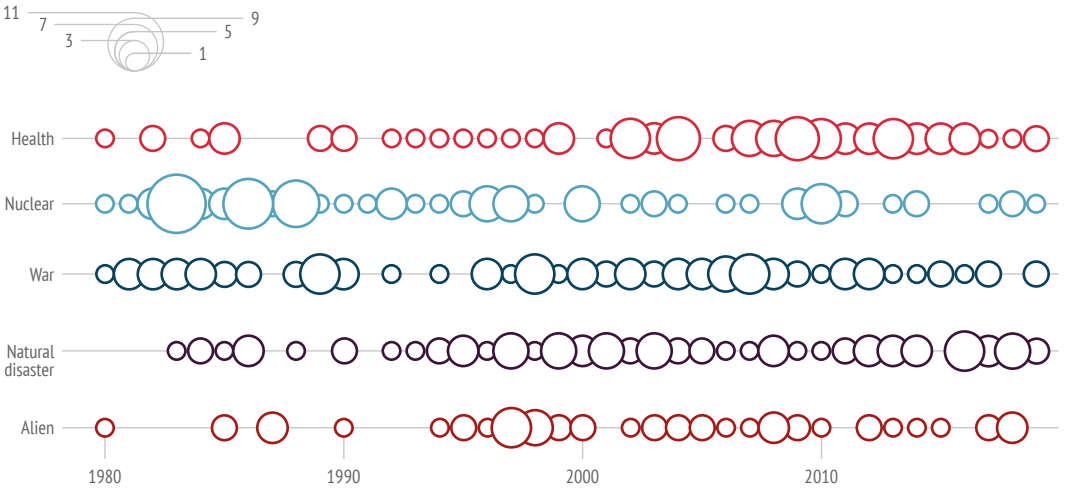
Data: Nicolas Minvielle, Rémy Hermez & Olivier Wathelet, *Du bon usage des imaginaires pour l'innovation de défense: L'exemple du combatant débarqué*, 2018

In conclusion: how far can we go too far?

How far is it possible to imagine warfare futures? Notions of multi-domain warfare are widely discussed in military literature. However, fantasy pushes the cursor much further by offering visions of conflicts that are literally off-limits, where civilian populations are targeted as much as military or state targets. *Genocidal Organ* (2007) thus describes a world where a researcher has found a way to trigger civil wars on demand through linguistics. The issues raised are complex and go beyond the keys to understanding current conflict. There is no real target or pivotal point to attack, with the entire population being manipulated at a quasi-genetic level.

This example of true 'fusion war' shows both the abundance and the limits of fantasy. While science fiction stories are fertile resources for

An analysis of 500 end-of-the-world fiction titles: a distribution over time



Data: "Preparing for the unknown: An analysis of dystopian fictions", *Making Tomorrow*, 2020

exploring the pitfalls of prospective approaches or for pointing out some of their limits, they are not necessarily neutral or unbiased. In seeking to go beyond the present, science fiction sometimes raises profound issues that should not be overlooked. What is left of 'face-to-face' conflicts in these imaginary worlds, which more readily focus on guerrilla warfare, cyber-technology, etc. and assume post-apocalyptic situations as a starting point? This literature also reflects the fears and anxieties of an era.

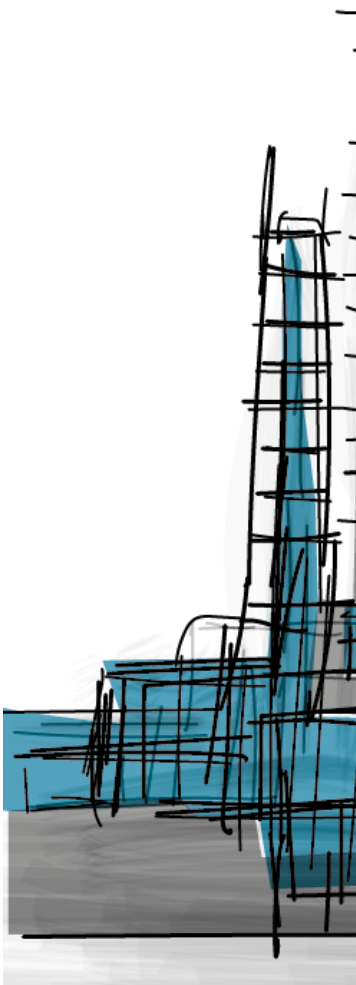
To be relevant, the approach we propose must rely on a large number of science fiction and fantasy novels in order to identify those that stand out from the rest, as well as to reveal the way in which these imaginative takes on the future evolve over time. Since these works tend to be mutually cross-fertilising, and have the potential to inspire forthcoming events, it is important to weigh up the value and likelihood of each of these imaginary versions of the future. These imaginative constructs of the future have the potential to confront us with alternative and challenging versions of what lies ahead. They are, finally, a magnifying mirror to help us take a step back from our own biased projections.

THE PEOPLE GO TO WAR: OF GRIEF AND GRIEVANCES

The people go to war: of grief and grievances

The following five scenarios share one particular feature: the active involvement of non-state actors. They therefore reflect the increased activism by civil society in violent conflict, a trend that started in the late 1990s. Protest against environmental degradation, technological progress and low wages drive these actors – classical grievances. But in these scenarios, non-state actors have resorted to new innovative methods of expressing their dissent, targeting cultural artefacts and objects, engaging in sabotage of oil infrastructure and using cyber tools.

The authors of these scenarios paint a picture where violence might not be highly lethal, but disruptive enough for states to be worried. The other feature we find in all five scenarios is that it is states that are held responsible for causing this violence in the first place: for not acting earlier on the energy transition, on socio-economic reforms or even foreign policy changes. The attentive reader will hence find ideas on how to prevent these conflicts from happening in the first place – a feature the other chapters in this volume do not necessarily offer.

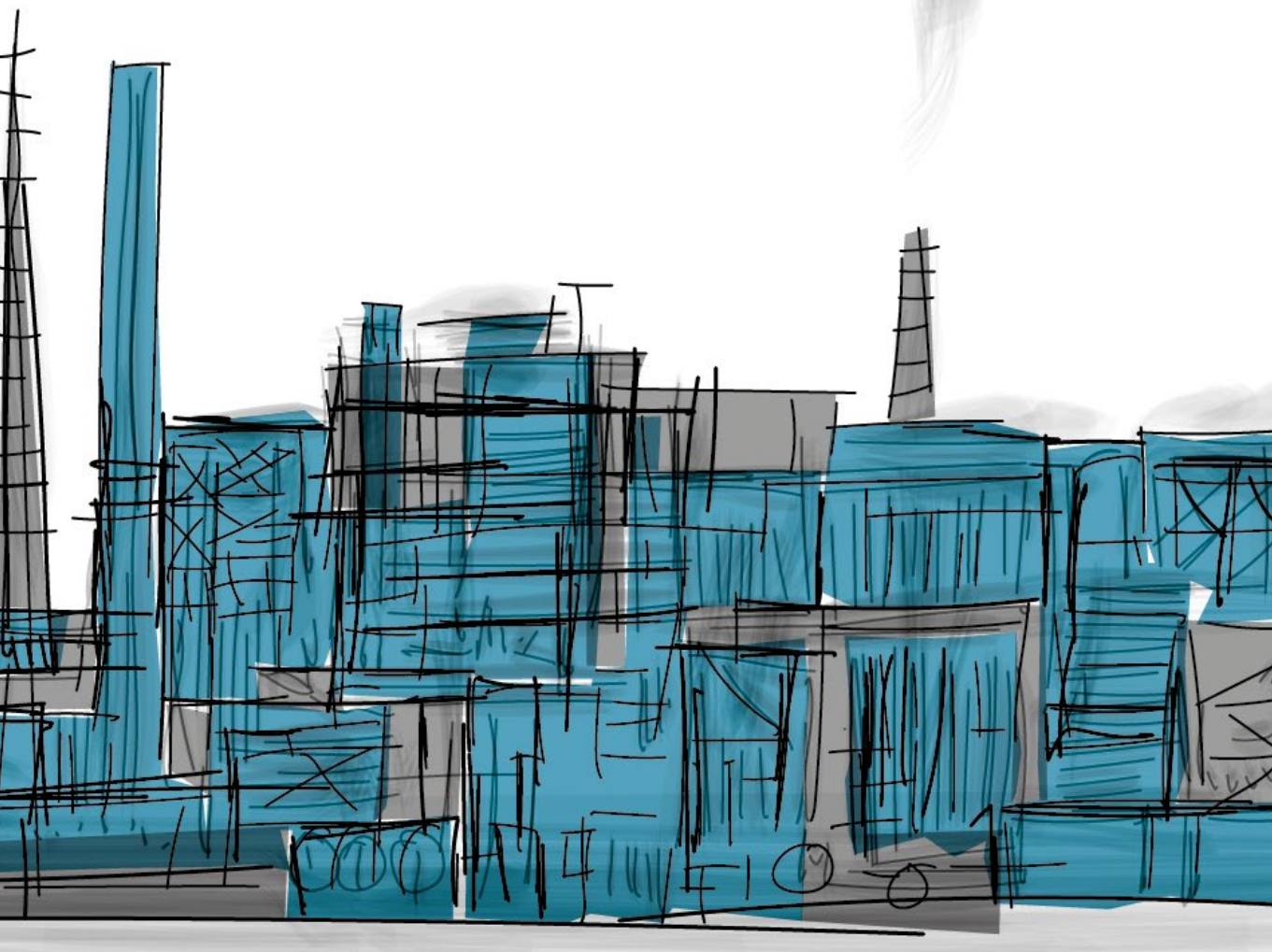


CHAPTER 1

MARX GOES GULF

The rise of the working class

by
ALI FATHOLLAH-NEJAD



Assumptions 2030

> Labour movements become transnational

> Global oil price has crashed

> Gulf relations are tense

> Governments crack down on protests

> China expands its footprint in Iran

"A mysterious series of widely heard explosions at petrochemical and oil plants have occurred early this morning on both sides of the southern part of the Iranian-Iraqi border. The fires caused severe damage to both countries' production output. Eyewitnesses reported unidentified armed groups clashing with security forces, and there are some reports that an Islamic Revolutionary Guards Corps (IRGC) military complex is also believed to have been stormed by armed men, despite official denials." This was the breaking news on Al Jazeera's morning programme on 14 June 2030. By lunchtime, the international oil market had reacted, tripling the price from $20 to $60 per barrel; Iranian officials accused 'the evil nations' of Saudi Arabia and Israel of being the perpetrators in a bid to weaken two crucial oil-exporting rivals at a time when its own production was disrupted after weeks of strikes. Baghdad remained more poised, making no concrete accusations beyond the usual pointing towards criminal networks.

After weeks of speculation about sabotage at the hands of anti-Iran powers, it became increasingly clear that an unexpected culprit was to blame: a new form of militant labour activism. Anchored in the region since the second half of the 2020s, activists had campaigned for years for wages to be raised above poverty levels. This act was the next escalatory step to signal to both states the immense capacity for disruption that they possessed. It also became clear that the damage to infrastructure in the energy industry had been strategically executed so that it could be repaired (thus avoiding the workers' own professional future being jeopardised) yet was dramatic enough to showcase the activist movement's capacity to wreak havoc.

...

A week before the above-mentioned explosions, angry Khuzestani workers stormed and destroyed a largely empty Chinese state firm's office in a night raid. This was no coincidence as China was seen as a key actor in the conflict.

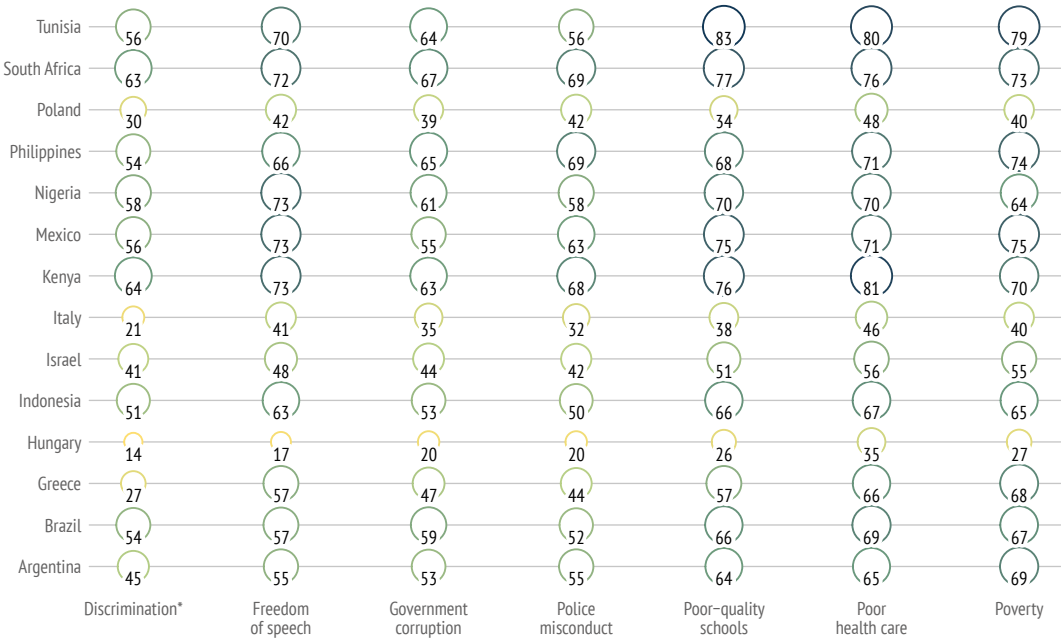
At first, Iranian workers welcomed the revamped JCPOA+ (a Joint Comprehensive Plan of Action centred on Iran's nuclear programme plus some regional geopolitical arrangements, especially regarding power-sharing in Iraq). But as Western oil giants remained cautious about re-entering Iran's oil industry, Chinese firms were the first to be granted access to Iran's resources in line with the 25-year strategic partnership between Tehran and Beijing. Much to the chagrin of the Khuzestani population, already suffering from disproportionately high unemployment (reaching 50% in some areas), Tehran acquiesced to Beijing's demand that the bulk of labourers working in those oil fields should be Chinese. Disgruntled workers began to organise in Khuzestan, but also in neighbouring Iraq, where the region around Basra had been the site of unrest for years.

These developments were not unique to Iran and Iraq: transnational labour movements had emerged all across the Middle East, including Egypt, Lebanon and Saudi Arabia – a process that slowly started in the early 2020s – setting up transnational coordinating councils with a common agenda and cross-border coordination of activism, primarily organised via social networks. Labourers lamented low wages of often as little as $2 per day, the extreme conditions under which they had to work and the lack of protection provided by the authorities as soaring temperatures of above 55°C led to over a thousand deaths among young Iranian and Iraqi workers, while their Chinese counterparts enjoyed better working and accommodation conditions.

In parallel, there was also a process of lumpenised radicalisation among parts of the working classes, with progressive revolutionary

Drivers of political activism

People who say they are likely to take political action, such as contact an elected official or participate in a demonstration, for each issue, %



Data: Pew Research Center, 2018

movements, such as the Iraqi-Iranian People's Council for Revolutionary Change, supported by leading public figures in both nations, as well as the highly nationalistic regimes, vying for their hearts and minds. These revolutionary movements – led by workers, students and women – were also able to make inroads into a widely impoverished middle class, through coordinated joint actions, such as the cooking-pot protests from home rooftops that took place every Friday night starting in 2027. This development aggravated regime concerns over a powerful intersectional alliance between the lower and the middle classes, whose socio-economic fate increasingly aligned – posing a serious threat to their rule.

In response, both Khuzestan and Basra provinces underwent a process of heavy securitisation during the 2020s as they were both hotbeds of anti-government popular protests and labour activism. This was a problem for Tehran and Baghdad because of their central role in providing both states with crucial hard-currency revenues. In Tehran, post-Khamenei Iran came under the rule of a more militarised and nationalistic establishment emerging from the ranks of the IRGC, with their former commander and ex-Speaker of Parliament, Mohammad-Bagher Ghalibaf, assuming the presidency and portraying himself as an iron-fisted nationalist moderniser. Despite a modicum of economic recovery after the signing of the 'JCPOA+', the socio-economic misery that plagued large parts of Iranian society continued to fuel protests, with demonstrators taking to the streets to reject the post-Khamenei military regime. These protests, however, met with brutal repression. In Iraq, popular activism, especially in the south, against an inefficient and corrupt élite had continued throughout the 2020s but failed to bring about substantial changes.

...

Following the explosions of June 2030, Iran's IRGC launched a severe crackdown on Khuzestani social and political activists, accusing them of having conducted those attacks on behalf of external enemies, arresting thousands

and sentencing over a hundred to death in expedited trial proceedings. On the Iraqi side, the army carried out a similar crackdown on anti-government activists, with human rights organisations pointing to collaboration between Iraqi and Iranian security forces. In the meanwhile, however, both sides' security forces began to fragment, with some of them joining the revolutionary movements. The reason for this was the heavy toll that deteriorating socio-economic conditions had taken especially on the rank-and-file and their growing sense of politico-ideological alienation, given that crackdowns had routinely affected their own neighbourhoods.

This stark repression then paved the way for further radicalisation of the popular movements. By 2032 they were regularly staging large-scale peaceful protests but also conducting violent attacks on security forces on both sides of the border and targeting key state and economic sites. One of these incidents included the occupation of a major oil and petrochemical plant by armed Basra activists, which after a week of heavy artillery fire ended in a bloodbath. While the transnational character of the protest movement has enhanced its effectiveness, a new series of pacts sealed by several authoritarian regimes has been able to prevent any changes that might pose a threat to their rule from materialising. In consequence, the situation in which socio-economically deprived populations are pitted against their militaristic regimes has resulted in a protracted stand-off, where neither side can successfully push back against the other, making this confrontation a constantly ticking time bomb.

CHAPTER 2

GREEN TERROR?

The environment fights back

by
KATARIINA MUSTASILTA

Assumptions 2030

> Environmental activism radicalises

> Russian militias interfere in third states

> Green conflict affects state relations

It was May 2030. Henriette had woken up to the distant sound of a low-flying drone. At first, she had not been sure about this, but now, as she ran down the hill with only two of her comrades running beside her, half waiting for a bullet to hit her, she was pretty sure it had been a drone. She imagined the others on the floor and wondered whether any of them were still alive, as she saw the first *GetAnywhere* rental car in the distance.

Earlier that morning, after dismantling their tent, Molly and Henriette had started preparing for the early morning meeting of the transnational 'Clean Energy Action Now!' (CEAN) core group. The group had convened near Tromso, Lapland, Norway, nearly three weeks after they had kidnapped Dimitri Sharpaneva, the new head of Gazprom's hydrocarbon activities in the Barents Sea. The action had started off as planned – Sharpaneva had been in Oslo for the crisis convention concerning the repercussions of the oil spill that had occurred in the Norwegian-Russian maritime boundary. However, he had been more heavily guarded than expected and a security guard had been lethally hit by a bypassing car amid the kidnapping. Both Norway and Russia had quickly declared CEAN as a terrorist organisation and the prime minister of Norway had sworn to bring the abductors to justice.

In the morning, just before she heard the first screams as she was walking towards the house, Henriette had been thinking about the events following the release of their video showing Sharpaneva reading the group's demands for his release: total cessation of all plans concerning exploration and drilling within the Arctic Circle; compensation for all the communities harmed by the oil spill; a realistic plan from both Norway and Russia for a total transformation of energy policy. In the two weeks that followed, it had become clear that CEAN members' anonymity had been compromised and that the Norwegian police were not the only ones looking for them: several homes of environmental activists believed to be CEAN-affiliated had been raided by unidentified groups of men, Henriette's own apartment in Oslo was ransacked and the head of the CEAN cyber-team had mysteriously disappeared from her home in Tallinn.

The cars appeared half an hour after Henriette had woken up. She saw three of them pulling down the small road and before she fully realised what was happening, six men wearing green camouflage outfits and carrying machine guns jumped out and headed directly to the front of the house. The firing started just after she heard the first screams, then paused for a few seconds, and started again. Henriette started running after the second pause, and it was only after she saw that *GetAnywhere* car, that she realised she was squeezing her phone with the filming app *Vidder* on.

As Henrietta finally reached the car with Molly and Jóse, she saw no sign of the camouflaged men nor did she hear the commands being relayed to them in Russian. Later that day, once they got their hands on new hardware, Henriette discovered the headlines stating that Sharpaneva had been successfully rescued from what appeared to have been a CEAN hideout on the outskirts of Tromso, during a law enforcement operation that resulted in twelve international terrorists dying after first opening fire against the police. Just as the identities and nationalities of the dead terrorists started appearing on social media, Henrietta was uploading a new video on *Vidder*, titled 'Our land under siege: foreign militia slaughtering environmental activists in Norway.'

...

CEAN was established in 2027, after the conservative party in Norway won the elections and immediately proceeded to allow Equinor to start production in the maritime boundary area of the north-eastern Barents Sea, which already hosted the Russian gas giant Gazprom which had first discovered the profitable oil reserves

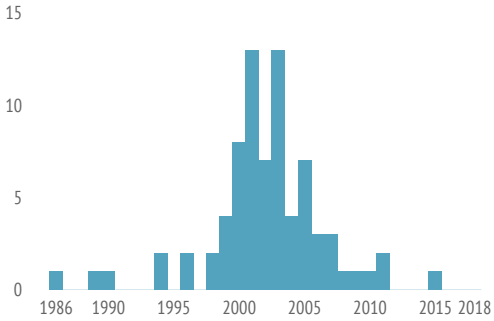
in the area in 2026.[1] While the potential of high returns for investments in the area had quickly incentivised Norway to demand its share of the discovered reserves based on the 2010 bilateral maritime agreement, there had been strong domestic opposition against Norway allowing any extension of petroleum activities by its state-owned oil company.[2] Ever since the pandemic at the beginning of the decade, polarisation between those in favour of extending exploration and drilling in the Arctic and those vehemently opposed to this had grown. Environmental organisations, indigenous Sámi groups, and many youth organisations argued that Norway was acting increasingly hypocritically – and unconstitutionally – by investing in hydropower and saving rainforests on the one hand while continuing to expand oil and gas production activities in increasingly vulnerable areas in order to maintain its main export source on the other hand.[3]

While established in Norway, CEAN was transnational from the start. Norway's new generation of environmental activists – particularly in the north where the Sámi communities reside – were tightly connected with environmental and indigenous activists in the Americas and sub-Saharan Africa. In Brazil, Colombia and South Africa, for example, groups defending their livelihoods, often based on customary land management regimes, had faced increasing insecurity and targeted violence by militia groups during the past two decades.[4] Describing itself as a radical unarmed group, CEAN focused on cyber operations at first, hijacking the websites of petroleum and mining companies, leaking classified documents of these companies, and launching big online campaigns to mobilise

Eco-terrorism

Attacks by environmental groups Earth First!, Earth Liberation Front, Earth Night Action Group and Sea Shepherd Conservation Society, 1986-2018

Eight of the attacks took place in the US, two in Canada, two in Mexico, and one each in Chile, Greece and Iceland.



Data: Global Terrorism Database, 2019

resistance. CEAN saw multinational companies as the main threat to both the fight against the worsening climate catastrophe and democratic governance overall. While the CEAN logo could occasionally be seen in climate-protests and demonstrations, it had no public leadership figures and its members retained their anonymity.

The situation escalated in autumn 2029, when a fire broke out on a Russian-owned oil tanker in the Barents Sea, leading to the century's worst oil spill and the loss of 33 lives. The spilled oil contaminated much of the transboundary fisheries but also reached the marginalised ice zone, with horrendous effects on its vulnerable

1 Norway's leading oil fields in the North Sea are drying up and the Barents Sea has been of increasing interest since the mid-2010s. Norway's Petroleum Directorate estimated significant reserves to be located in the north-eastern part of the Barents Sea, adjacent to the maritime border of Norway and Russia. See "Plenty of more oil in Barents Sea, says petroleum authority", *The Barents Observer*, February 24, 2020, https://thebarentsobserver.com/en/industry-and-energy/2020/02/plenty-oil-barents-sea-says-petroleum-authority.

2 The 2010 maritime agreement between Norway and Russia sets a framework for sharing resources spanning the border region. Norway's Petroleum Directorate indicated in 2019 that Norway would demand a share of the resources if Russia made discoveries in the areas it was exploring. See "Norway ready to claim share of any Russian Arctic oil and gas finds", *Reuters*, January 10, 2019, https://www.reuters.com/article/us-norway-russia-oil/norway-ready-to-claim-share-of-any-russian-arctic-oil-and-gas-finds-idUSKCN1P41VX.

3 "Norway faces climate lawsuit over Arctic oil exploration plans", *The Guardian*, October 16, 2016, https://www.theguardian.com/environment/2016/oct/18/norway-faces-climate-lawsuit-over-oil-exploration-plans.

4 "More than 1,700 activists have been killed this century defending the environment", *The Conversation*, August 5, 2019, https://theconversation.com/more-than-1-700-activists-have-been-killed-this-century-defending-the-environment-120352.

ecosystem.[5] In response to the immediate environmental destruction that followed, mass demonstrations were held in all Nordic countries and major Russian cities against the alleged mismanagement of the difficult conditions in the Barents Sea leading to the catastrophe. The incident caused opposition against oil production in the Barents Sea to surge, and the Norwegian government temporarily halted any developments in this regard. Russia, in contrast, made no such pledges.

Nearly a year later, as the two countries prepared for another crisis convention in Oslo to decide on further measures to alleviate the long-term destruction caused by the spill, CEAN was finalising plans to move to direct action. Their plan was to make Sharpaneva an example of a humiliated – but physically unharmed – oil magnate stripped of his power, with daily newsflashes anchored by Sharpaneva himself informing the masses truthfully about the environmental impact of his industry.

Yet CEAN grossly misjudged the extent to which Gazprom was able to operate internationally. Gazprom's private security firm was sent out to Norway hours after the kidnapping and Norway's appeals to Gazprom and Russia to abstain from conducting law enforcement activities on Norwegian territory were weakened by lack of domestic consensus over the exact nature of Gazprom's security firm and threats from Russia to dismantle the 2010 maritime agreement altogether. Having learned about the raid against the alleged CEAN safe house where Sharpaneva was kept only minutes before it took place, the prime minister of Norway made a hasty call to assume agency over the raid, in order to cover the presence of a fully armed Russian militia group in Norway. This made the aftermath of the leaked video footage of the event considerably worse.

...

The video footage from northern Norway sparked massive protests all around the country, mobilising widely across societal groups. While the majority of Norwegians still disapproved of the kidnapping, CEAN's aims were supported by many and only a minority regarded the actions against them as just. The protesters demanded the resignation of the prime minister, who had failed to impede and then tried to cover up extrajudicial executions on Norwegian soil by a Russian private paramilitary group. The protests were mostly non-violent, yet there were signs that some groups involved – radical left and right – were instigating rioting.

In addition to the mass protests, the killing of twelve CEAN members caused major international turmoil. There were seven nationalities among those killed, including two individuals from Norway's NATO allies. Brazil and Sweden recalled their Russian ambassadors after a few days of escalatory rhetoric, during which Russia continued to deny any role in the operation to rescue Sharpaneva, and Gazprom claimed that their security officers had followed the instructions of the local authorities. In Finland, popular street protests demanded an end to Russian oil imports, and diplomatic tensions escalated between Helsinki and Moscow to a level unseen in the twenty-first century. For the EU as a whole, the incident proved another test of its internal cohesion: some member states, e.g. Sweden and France, demanded that sanctions be imposed on Russia for interfering in Norway's sovereignty while others (the Netherlands, Hungary) opposed this.

Just as the civil unrest across Norway and elsewhere was beginning to die down, the Tallinn police discovered a body later identified as that of the head of CEAN's cyber team in a forest near her home. The body showed signs of torture. The following Saturday, protests driven by both environmental and rule of law concerns resumed on an unprecedented scale across European cities and beyond and the international crisis escalated.

5 The marginal ice zone refers to the area where Arctic sea ice meets the open ocean. The area is home to a rich biodiversity such as various planktons, fish, polar bears, birds, seals and whales. The World Wildlife Fund (WWF) states that "an oil spill could potentially cause a collapse of the entire food chain with an impact on the wider Arctic region that depends on the biological productivity of the marginal ice zone": WWF, "Arctic lifeline could be cut by expanding off-shore oil drilling", April 27, 2020, https://arcticwwf.org/newsroom/news/arctic-lifeline-could-be-cut-by-expanding-off-shore-oil-drilling/.

CHAPTER 3

THE DIGITAL ROAD TO 'HELL'

The people versus tech

by
STANISLAV SECRIERU

Assumptions 2030

- > Russian society becomes increasingly high-tech
- > There is growing resistance to this phenomenon
- > Elements within the Russian Orthodox Church become radicalised
- > Non-state actors master cyber methods too

Father Mefodiy, the spiritual leader of an aggressive anti-technology movement, was delivering his last sermon shortly before the monastery was stormed by the elite special intervention unit Alfa. Dressed in black, he stood with a white wooden cross in front of around 500 monks armed with Kalashnikovs, Cossacks, hard-core members of the radical Holy Russia sect and other pious supporters. Outside the gates, the Alfa fighters dressed in Iron Man-type bulletproof suits and armed with laser rifles were taking their assault positions. Dozens of mini-drones were hovering like wasps above the monastery providing real time video feed into the augmented reality helmets of fighters; the inbuilt AI instantly calculated and displayed the best trajectory of attack. The years-long stand-off between an extreme version of traditionalism and post-modern authoritarianism was about to reach its climax.

"Have no fear brothers and sisters!" Mefodiy exclaimed. "These techno-Satanists may take our lives, but they will never be able to take our souls." He continued: "Do not be afraid, brothers and sisters! Our cause is the right one, the liberation of Orthodoxy from the rule of demonic algorithms. Our sacrifice today is not the end, but the beginning of revolt, which like the Genesis flood will wash away this sinful regime with all its computers, machines and Chinese research labs. Brothers and sisters, do not be afraid to shoot! We know that Jesus Christ preached that if anyone slaps you on the right cheek, turn the other cheek. But those who have gathered outside the gates are not humans but malign robots who have come straight from hell. The commandments of the Son of God do not apply to them. Now, take out your swords and do not rest until you defeat the dragon of darkness who has subjugated our holy land and seeks to destroy our millennial way of life!"

Alfa was given the order to proceed. A bloodbath followed; after a 2 hour shoot-out, more than 273 people were killed, among them Father Mefodiy. While anti-technology crusaders despised technology, they did not hesitate to use it to recruit supporters and inflame anti-government sentiment. Shortly after the assault, Orthodox militants hacked the Sber-glasses servers,[1] which provide ubiquitous internet connectivity to more than 100 million Russians wearing them, and streamed the recording of the sermon and the subsequent ruthless suppression of the mutiny in the monastery. Before playing the recording with the help of deep fake software they added 15 extra seconds showing how troops implanted the chips in the bodies of survivors.

The next day, underground cells of the anti-technology movement across Russia sprang into kinetic action too, targeting symbols and infrastructure of the post-modern age. Several Huawei AI research labs and two major internet traffic exchange points in Moscow were set on fire. Dozens of commercial drones loaded with mini-explosives hit 5G towers across the country. The country's law-enforcement apparatus, which was heavily reliant on IT technologies for surveillance, was virtually crippled. In the capital a crowd of a few thousand religious radical supporters ransacked the building of the Ministry of Digitalisation and Sber's office which hosted the biggest store of private data collected through Sber-glasses. Nationalist mobs and angry losers of the digital revolution opportunistically joined the revolt. They attacked the Chinese embassy and looted

1 In the 2010s the Russian state-owned bank Sberbank became increasingly integrated into the IT sector. In 2020 it underwent rebranding, dropping the word "bank" from its name, and remaining just "Sber".

shopping malls. Violence and chaos spread to a few more cities. Russia became the theatre of the first major urban anti-technology revolt of the twenty-first century.

...

Throughout the 2010s the country's political leadership and the Russian Orthodox Church had joined forces to clamp down on aspirations for liberal democracy in Russia and promote a combative foreign policy. This close partnership was mutually advantageous. While the state aggressively persecuted any alternative Christian movements which sought to challenge the Orthodox Church's primacy on Russian soil, the church called for defence of traditional values, endorsed anti-Western conspiracy theories, sprinkled missiles with holy water and justified Russian military campaigns abroad as 'holy wars'. As a result the Orthodox Church, an already very conservative institution, had by 2020 veered to the extreme.

Soon however cracks started to emerge within the church between pragmatics, ready to support the state's agenda in exchange for institutional or personal perks, and ideological radicals, intent on pushing for extreme traditionalism no matter what. Militant factions pressurised Moscow's Patriarch and the political leadership, perceived as too moderate, to aggressively defend the moral purity of the country and clamp down further on foreign cultural influences. These factions gained some traction in society; semi-clandestine Orthodox organisations actively defending the traditional way of life and promoting the vision of a Christian state started to proliferate outside of the Kremlin's control. They were behind the increasing number of bomb alerts in 2021-2022 at cinemas and theatres running shows which were deemed as insulting the religious feelings of Russians. Several *avant-garde* art studios were burned, while more and more painters, film directors and actors were physically attacked. This all culminated in the assassination of a young rising female star after she appeared in a few nude scenes in a Russian historical blockbuster about Alexander Nevsky.[2] This was too much for the Kremlin; the partnership with the church was mutually advantageous but never one of equals. Religion was supposed to be 'the opium of the people,' as per Karl Marx's famous dictum, whose dosage the Kremlin firmly controlled. And priests were supposed to play by the Kremlin's playbook and not to morph into self-standing entrepreneurs of violence.

Moreover, the country's leadership was reevaluating the utility of religion as a political tool, as in the early 2020s religious issues turned into an unnecessary irritant in big urban centres, where the authorities were fast losing popularity and support. In these conditions, for the Kremlin, increasingly captivated by the numerous opportunities digitalisation offered for social control, the alliance with the Orthodox Church gradually lost its former appeal. Instead, digitalisation became the new religion. Cyber technologies were expected on the one hand to deliver better services to citizens (thereby increasing their levels of satisfaction and making it easier for the authorities to keep the population mired in political apathy). On the other hand, these served to enhance the state's capacity for electoral fraud (e-vote), surveillance and more surgical repression (reducing the possibility of a popular backlash). Still under Western sanctions, Russia opened up more to Chinese companies and their know-how to speed up digitalisation; 5G and elements of a social credit system appeared in Russia in 2025-2026.

The Kremlin tried to put the Orthodox genie back in the bottle. It deployed cyber capabilities as well as kinetic force to stave off unauthorised religious-driven violence. More fake videos were circulating on SberTube and state TV channels allegedly presenting dissenting prelates engaging in homosexual acts. Subsequently, the church stripped rebel priests of

2 Alexander Nevsky (1221-1263) was Grand Prince of Vladimir and Novgorod. He was canonised as a saint by the Russian Church in the sixteenth century.

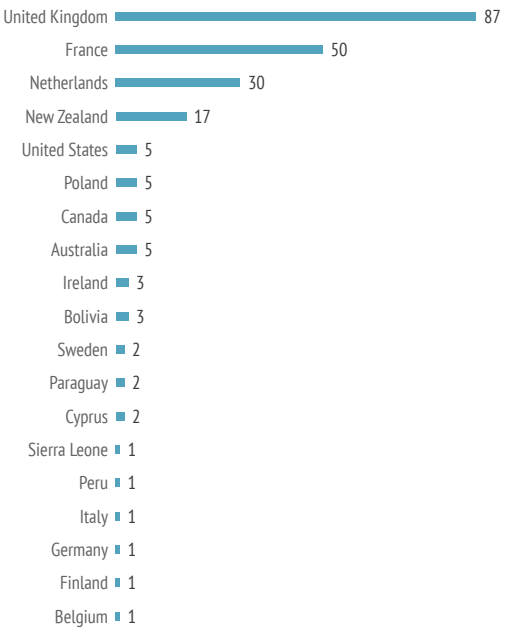
their titles and positions; those who refused to vacate monasteries or churches were removed by riot police. Security forces detained the leaders behind bomb alerts and attacks. Several were found dead in prison; officially, they had committed suicide.

But instead of suppressing militant Orthodoxy, the 'no-man-no-problem' approach pushed it underground and it became even more radicalised in the second half of the 2020s. For Orthodox zealots, those who had been detained and killed were likened to new martyrs. Russia's state marriage with technologies and their use against Orthodox prelates advocating a greater role for religion and traditional values in society mobilised radicals against the government and its foreign backers. They metamorphosed from crusaders for moral purity into campaigners for emancipation from technologies. In their ideological struggle, zealots recycled conspiracy theories, only this time, these were targeted against their own government and China. The info space was flooded with stories that the state campaign for vaccination against Covid-19 masked a plot to plant chips in the human brain, so that the government could experiment switching people on and off when needed. In the same vein, rumours abounded about tests on humans in the Chinese AI Research Labs that were springing up throughout Russia.

The radicals worked to widen their appeal. They called on disgruntled Cossacks to join their ranks against the regime which had betrayed their Orthodox brothers in Donbas by not pushing military operations deeper into Ukraine and refusing to recognise the 'people's republics'. They also tried to reach out to victims of technological unemployment and urbanites increasingly unhappy with the state's drive to digitally control their private lives. The appeal of the anti-technology discourse was reflected in public surveys according to which 69% of Russians wanted the government to limit digitalisation in order to save jobs and restore the shrinking private space. It was even rumoured that some pious high-ranking state officials were sympathetic to the radicals' cause and had leaked information to them about the government's planned crackdown operations.

5G masts under fire

Arson attacks on telecom infrastructure by anti-5G groups as of October 2020



Data: Telecom association GSMA (as cited in *Politico*), October 2020

By the late 2020s the movement had extended its reach (comprising 50 active cells around Russia), and become more clandestine and better organised. Although it did not represent the majority, it was nevertheless a very vocal, dangerous and aggressive minority, which had the potential to mobilise a growing number of technophobes and radicalise those who had lost out in the digital revolution.

Father Mefodiy, a mystical monk who allegedly talked to the souls of the dead and could see into the future, emerged as spiritual leader of a hydra-like anti-technological movement. He claimed to have been sent on earth to stem the advancing tide of technology which would destroy Russia and its entire civilisation. The only way out was to halt current work on innovation and annihilate existing digital infrastructure.

Orthodox zealots organised the first violent protests in front of the Chinese embassy and Sber's central office. Angry crowds chanted "We are not your guinea pigs!" Radical Orthodox activists then sent letter bombs to

research labs in Russia where scientists were working on quantum computing and neurointerface projects. Also in the late 2020s a first attempt took place to damage 5G towers by using a suicide-bomber. This escalation forced the authorities to ban Mefodiy's sermons from being distributed via social media and urgently track him down. Based on a tip from an informer, the authorities found out his whereabouts and rushed to prepare a raid on the monastery which was in a remote and inaccessible location. It seemed that his core supporters were hiding under the same roof. The security forces mounted the assault hoping to decapitate the movement in one strike and severely disrupt its future operations. However, this was a trap; the informer was in fact part of the cult and the invitation to the bloodbath and its streaming online was orchestrated to serve as a latter-day echo of the first salvo of the cruiser *Aurora* in 1917,[3] now signalling the beginning of a large-scale anti-technology revolt.

...

After absorbing the initial shock of surprise the government deployed the National Guard on the streets. Hospitals received more than 2,000 patients suffering severe damage to eardrums and eyes as the soldiers resorted to the extensive use of sonic cannons and flash grenades to disperse crowds. Although a modicum of order was restored in the capital and other cities after a few weeks, Orthodox militants resorted to hit-and-run tactics, carrying out attacks on digital infrastructure, IT companies and their staff. The internet was still slow, online banking functioned only intermittently, and many e-government services were suspended. Society was in a state of shock and feared the worst; there were no public demonstrations in support of the regime, while few openly expressed support for the violence induced by anti-technology rebels. Yet, on Russian social media the hashtag #No2DigitalizationWithoutHumanFace was trending for weeks. *Rossya24* ran reports about an externally-inspired massive hybrid intervention in Russia.

China evacuated personnel from its embassy and all employees from Huawei Labs; IT companies began to leave Russia. In anticipation of attacks, a dozen leading Russian researchers departed for Silicon Valley. However, they were not completely safe there as the events in Russia reignited a violent technophobia movement in the US. Half a year later, a letter bomb exploded at one of the facilities producing experimental devices for the 6G network. It was the first act of anti-technology terrorism in the US since 1995. Shortly afterwards, the magazine *Wired* received an anonymous message warning that more attacks would follow if the work on 6G was not completely stopped. In Russia, the economy nosedived, the idea of digitalisation was discredited for years to come, the church was deeply divided, and another wider social explosion was liable to erupt any time soon. International investors panicked and started a massive selloff of Russian sovereign bonds. It was once again a make-or-break moment in Russian history. A group of relatively young senior officials from the power institutions were determined to bring the situation under control. And to do this they began to plot a palace coup to overthrow the 78 year-old president who had run Russia for the best part of three decades.

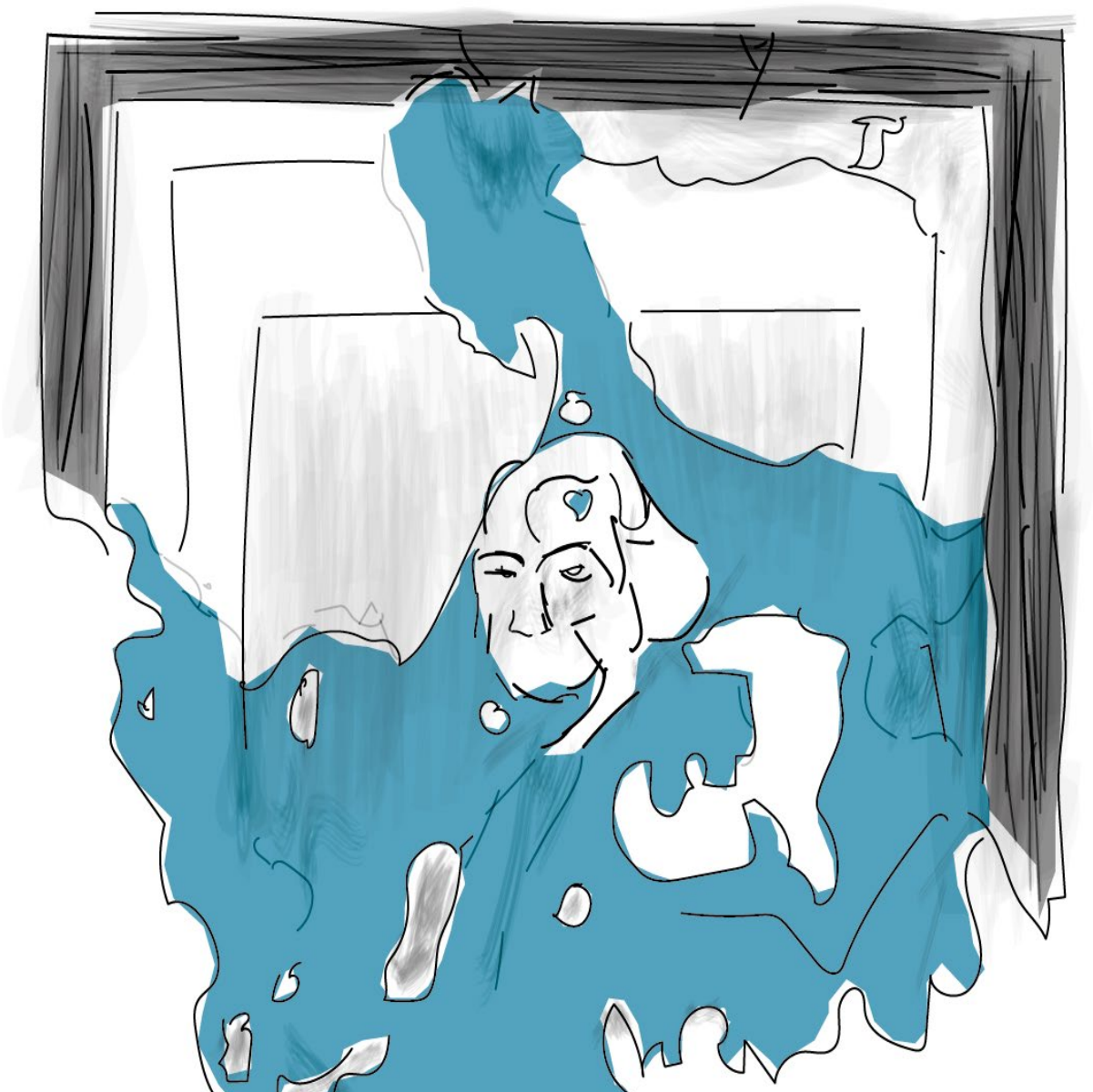
3 One of the first incidents of the October Revolution in 1917 took place when the cruiser *Aurora* reportedly fired a blank shot from its first canon, giving the signal for the attack on the Winter Palace.

CHAPTER 4

INSTANARCHISTS.COM

Culture in the crosshairs

by
TOBIAS PIETZ



Assumptions 2030

- Cultural objects become the targets of new radical as well as older terrorist groups
- Government inaction on climate change leads to radicalisation of environmental movements
- States are at a loss to protect culture against vandalism

Marie Thibaut took a deep breath. It was always hard for her to pass this spot in the museum since the attack. Almost like before, a huge group of visitors were standing in front of it, blocking the view. But she knew that there was nothing to see any more. Well, actually, that was not strictly true. The director of the Louvre had decided to preserve the scene just as it was after the attack. Not much remained when at 5am on Earth Day, 22 April 2025, a young woman named Manola Varese inserted two litres of highly concentrated sulphuric acid into the picture's air conditioning system. Goppion, the Italian company belonging to Varese's father, had built the glass box protecting the painting. The whole operation was made possible because of the involvement of two other members of the group Extinction Rebellion – the son of the Louvre's general administrator as well as Antii Sairanen, a young engineer at Vaisala, the company in charge of regulating the air temperature surrounding the painting. That day, the Mona Lisa vanished forever as the destruction was beyond repair. Five years after the incident, people were still waiting in long lines to have a look at the void.

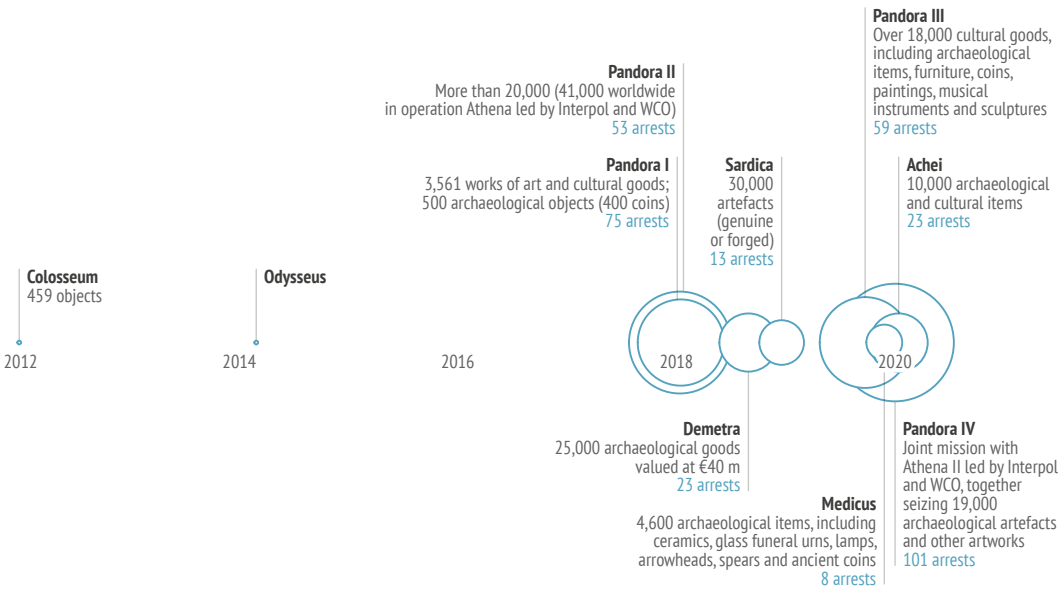
By today, 22 April 2030, over 300 key artefacts and pieces of art as well as 20% of the sites on the World Heritage List are gone, either partially or completely destroyed or (in the case of artefacts) sold on the black market. Moreover, many groups had identified smaller museums and regional collections of art as easy targets as these lacked sophisticated security systems but still held valuable assets and had high symbolic meaning for regions and communities. By 2030, about 10% of the roughly 50.000 museums worldwide had been attacked or plundered in incidents clearly inspired by what had happened in the Louvre.

Earth Day 2025 marked the beginning of massive destruction and plundering of cultural heritage. Under the motto "If you destroy our future, we'll blow up the past" hundreds of young people, mostly former members of the two popular environmental movements 'Fridays for Futures' and 'Extinction Rebellion;' went underground and formed a violent resistance group, targeting various cultural artefacts and sites – from pieces of art to monuments or historic properties. Even festivals were a target such as the famous opera festival in Bayreuth where a group succeeded in planting "Skunk", a malodorous, non-lethal weapon stolen from the Israel Defence Forces (IDF), under the front row seats at the opening on 26 July 2025 with 10 heads of states and various ministers and representatives of Western elites affected and stained for months afterwards.

European governments were appalled but who would have imagined that by 2030, the rebellion would have moved from acts of vandalism to actual lethal violence and have transformed from a European into a global – albeit quite diverse and contradictory – movement? Attacks, acts of vandalism and destruction and violence took place across the world, from Egypt to China, from the US to Australia. At the outset, on 4 July 2026, a group in the US calling themselves "!nstanarchists' were able to destroy a rare copy of the Declaration of Independence while live-streaming it via Facebook with the hash-tag #heritagedestroyed. For the destruction of the bust of Nefertiti, an inside job similar to what had happened at the Louvre, radicals had recruited the teenage daughters of the head of the Neues Museum in Berlin who were allowed to be present when the bust was being cleaned, and then grabbed and shattered it on the marble floor of the museum. Altogether, more than a dozen iconic cultural objects and properties were destroyed through such tactics during the first two years, with the attacks listed and celebrated on websites such as heritage-destroyed.tv or instanarchists.com. Even more pictures of demolition or vandalism of artefacts in local museums or of monuments were posted

Artefact trade in Europe

Europol operations targeting illicit trade in cultural goods in Europe



Data: Europol, 2020; European Commission, 2018

there, making the experience of lost cultural heritage not only a global but also a local and personal phenomenon for many people.

But when the same hashtag was used the following year by an Uyghur group who blew up the better part of the Terracotta Army in the mausoleum of the first Chinese Emperor in Shaanxi, observers realised that something was changing. Until then, militant groups had been demanding actions in favour of environmental protection and sustainability, trying to pressure governments to fight climate change and to prevent the destruction of biodiversity. Now, claims for independence or democracy were added to the list of grievances, not only in China but also in Egypt, where another group detonated a bomb in front of Cairo's famous Grand Egyptian Museum with the aim of undermining the Sisi regime's most important source of revenue, tourism.

With various groups threatening – for different reasons – "to bomb our way down the whole list of world heritage sites", UNESCO issued a global call in 2028 to all radical groups to stop destroying cultural heritage as it "is our legacy from the past, what we live with today, and what we pass on to future generations. Our cultural and natural heritage are both irreplaceable sources of life and inspiration."

By 2028, the remnants of the so-called Islamic State (IS) saw an opportunity in also hijacking the movement's global fame for their own purposes and revenues. Within one week in June 2028, the Al-Khazneh temple in Petra, the Temple of Bacchus in Baalbek and Persepolis in Iran, all UNESCO World Heritage Sites, were destroyed – these highly visible and symbolic attacks put the IS back on the map and into the news. Unlike the radicalised environmental groups, the IS actually did not destroy everything but secured key artefacts and sold them on the black market. It also started to infiltrate some of the European Instanarchists groups and thus laid its hands on even more antiquities to sell. Within a year, IS had reclaimed its leading role in global terrorism.

...

In March 2025, 22-year-old climate activist Greta Thunberg declared her battle against climate change lost, stepped back from 'Fridays for Future' and disappeared. What followed

were intense debates within the FFF, culminating at their yearly online summit in fierce arguments about how to proceed. Delegates representing both FFF and Extinction Rebellion chapters claimed that the only remaining option was a violent uprising. After two days, the whole movement broke apart and a small but vocal minority declared their intention to move underground to orchestrate a rebellion.

Cultural heritage, especially at the local level, had been an easy target for these radical groups as many regional museums or monuments lacked the needed security measures or awareness to prevent attacks or plundering. There were just not enough resources or personnel to secure the huge number of museums and monuments in the world from this global wave of destruction and vandalism. Frustrated by the failure of world leaders and governments to move towards carbon neutrality, the young and highly-motivated climate activists turned to radical acts of destruction and violence. Cultural heritage reflects and shapes values, beliefs, and aspirations, thereby defining a people's national identity as well as providing a sense of belonging, unity and personal identity to every individual. To destroy a famous monument or to vandalise a small city's museum therefore has an impact on both communities and individuals, especially as social media channels facilitate the worldwide and instant dissemination of images of such destruction. That is what radicals exploited. Moreover, this focus on cultural heritage provided huge revenues for terrorist groups who became freeloaders on the 'Instanarchist movement' and traded large amounts of artefacts from conflict-affected countries as well as smaller Western museums and collections.

...

The original Western groups of the movement were worn out and frustrated by the meagre impact their actions had had on global climate policies. No longer able to rely on public support in their own countries, most of them gave up and sought amnesties. Some of the most radical members joined other militant groups. Global warming and extreme weather phenomena hit Europe with droughts and high temperatures. The IS now dominated the global illicit trafficking of cultural goods and property, which enabled it to quadruple its revenues between 2028 and 2030, while museums worldwide struggled with the loss of artefacts as well as dwindling numbers of visitors. In 2005, more than 15,000 museums in Europe attracted more than half a billion visitors and generated not only ideas and learning opportunities but also employment and revenues – now a third have closed for good with unforeseen impacts on communities, education and identity.

CHAPTER 5

CHICKENS COMING HOME TO ROOST

Mercenaries strike back

by
SINIKUKKA SAARI

Assumptions 2030

- Hackers join militias due to external/ personal pressures rather than for financial reward
- They have the capacity to conduct lethal cyberattacks
- Russia is overstretched militarily in several theatres

"I have been an outcast as long as I can remember; many of us have a background like mine. The 'lords of darkness' have basically taken advantage of me since I was a teenager", said 'cyber guerrilla' Andrei – aka 'Kropotkin' – in the video recording. The shadowy figure continued bitterly: "They have made fortunes while I have slaved for them and got nothing for myself. Even worse, many of my comrades have been sent to jail or assassinated because of all the dirty secrets they know about the system. And Ilya here... Ilya's friend called for re-enforcements but was left behind and tortured and decapitated in Syria. The family got nothing – no compensation, nothing only intimidation and threats to make them keep their mouths shut. Instead those scoundrels were only interested in getting oil from Deir Ezzor and became even richer. How is that for loyalty?"

"Now we are taking them down with us – we'll bomb their gas pipelines, we'll bring down their banking systems and their money laundering schemes in the Caribbean. We'll burn their Chelsea mansions and Maseratis. We'll expose them all and then we'll destroy the whole rotten system! We'll take revenge in the name of our lost friends and our broken lives – this is war, and we have nothing to lose." Ilya walked towards his friend and joined the conversation: "It's exactly like Comrade Kropotkin says. My grandfather used to tell me when I was a kid that we proletarians have nothing to lose but our chains! We mercenaries and hackers are today's slave workers doing the dirty jobs for the evil guys in power who pretend to be patriots, but are only interested in getting rich themselves. But it's all over now! We will incite the masses to rise against the liars who rule us!"

A series of bombs, assassinations and devastating cyberattacks had shattered the equanimity of political elites in Russia and in the Western world. The main target had been the Russian leadership and the Russian economy. The ugly truth about the Russian leadership's illegal activities at home and abroad was revealed as hundreds of documents were leaked to the public and widely distributed. The NordStream underwater gas pipeline exploded as a result of a hacking strike that increased the pressure inside the pipe. Russian society polarised quickly as the leadership resorted to tough measures to root out the violent guerrilla movement. The country was in mayhem with little trust in either of the sides.

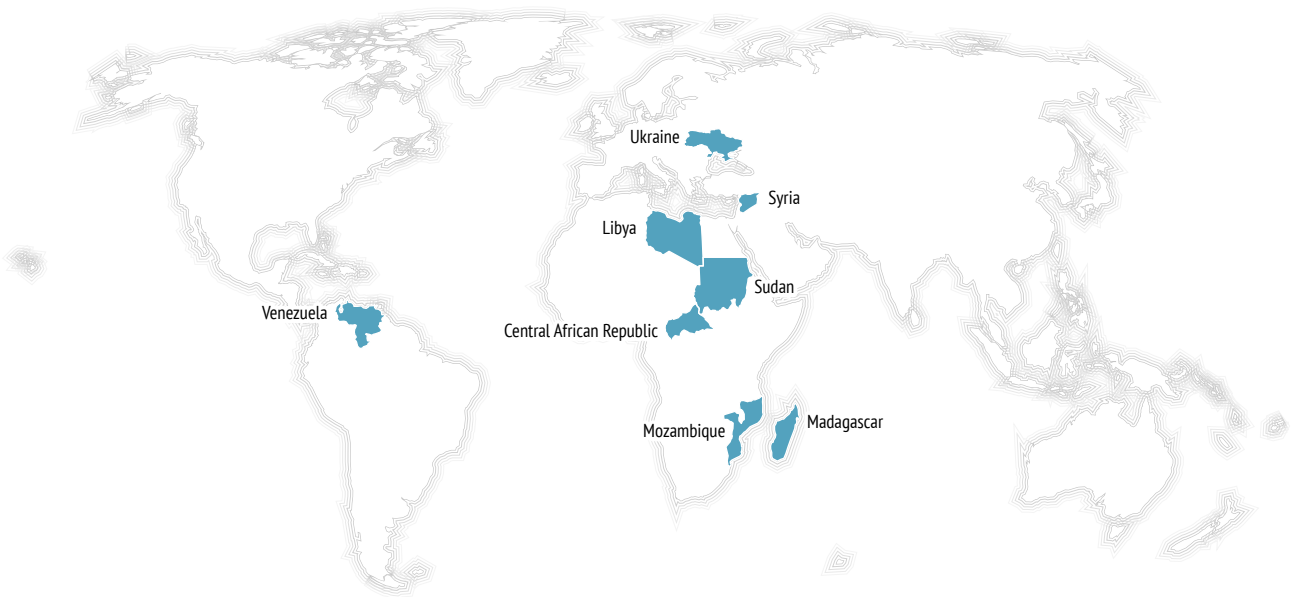
...

Since the mid-2010s, Russia had increasingly relied on the services of private mercenaries and hackers in its covert foreign operations which it wanted to conduct secretly, and for which it sought to deny responsibility. Many of the mercenaries and hackers had criminal backgrounds, or severe personal financial issues or were in danger of having their businesses confiscated by the state, so cooperation with the security services and state-supported Private Military Companies (PMCs) were not always entirely voluntary. The only way to avoid long prison sentences or personal bankruptcy – or something even worse – was to risk one's life fighting in Russian proxy wars abroad either on the ground or in cyberspace. In the early 2020s, the conflicts in Libya, Syria, Ukraine and in the Central African Republic (CAR) came to a head almost simultaneously while the Russian economy and Putin's succession plan for 2024 were derailed.

Politically – and perhaps psychologically – it was impossible for Putin to admit that he had made drastic mistakes in his policies and that it was time for him to leave the scene. Instead of taking responsibility for his bad decisions, Putin desperately hung onto power. Not only did he continue but he intensified the proxy wars Russia could no longer quite afford. Future historians dubbed the period the 'Dead Cat's Bounce' – just before the total collapse of Russian military interventionism, Moscow had resorted to extremely intensive fighting in all of

Wagner Group whereabouts

High-probability cases



Data: Foreign Policy Research Institute, 2019; Ifri 2020

the theatres simultaneously. Excessive hubris on the part of Russia's longest serving leader of all time was likely to have contributed to the chosen course of action.

After the mid-2020s, more and more fighters were recruited but they only had minimal training due to the shrinking economic resources of the Russian Federation. The equipment used was also of low quality – usually out-of-date malfunctioning Soviet weaponry. The casualty rate among the fighters was high and the rumour circulating among the mercenaries was that the state preferred to have them killed in action rather than return to Russia where they would easily become a dangerous liability for the elite. The compensation and status of mercenaries decreased year by year, which impacted negatively on their motivation. Abuse and human rights violations committed against locals but also within the proxy army units became the rule rather than the exception. Also numerous video clips where local rebels were shown torturing Russian fighters made the rounds on the internet. Working for the Russian PMCs became socially stigmatised; most Russians did not want anything to do with them or even to acknowledge their existence.

Due to Russia's shrinking economic assets, but also the increasing digitalisation of militaries and militias, the authorities also considerably expanded the 'cyber army'; it was considered the most resource-efficient form of fighting. Also virtual fighting became considerably harsher and bloodier over the years. Hacking tasks were more geared towards producing kinetic effects on the ground: hackers decoded foreign weapon systems and directly caused thousands of casualties by changing the target coordinates of missiles and hijacking drones. Refugee camps were typical targets, creating enormous human suffering and political upheaval in various parts of the world. After these types of operations became standard practice, many hackers became disillusioned and demoralised; it was one thing to steal documents and leak some incriminating details about someone you did not know in public, and quite another to actually kill civilians – even if from a distance – in a brutal conflict. Through these 'integrated proxy operations', the links between hackers and mercenaries became tighter; they often operated in small teams consisting of military and cyber experts.

Around 2026 a revolt began to simmer and quickly gathered pace within the ranks of the

mercenaries and cyber fighters who felt themselves to be outcasts. Andrei aka Kropotkin – a hacker who was interviewed in a legendary documentary film shot in 2028 – became a demagogue and the commander of a guerrilla cyber army. His friend Ilya – who was also shown in the film – directed the guerrilla war on the ground. Together they united the mercenaries and hackers for a common cause: extreme anarcho-communism. Since the coronavirus outbreak in the early 2020s, many anti-capitalist movements had gathered pace globally and nineteenth-century communist thinkers experienced an unexpected revival. According to Andrei aka Kropotkin's anti-capitalist worldview, it was not just Putin and the rotten Russian system that was to blame. In fact, Andrei and his followers blamed the Western financial institutions as much as what he called Russian 'oligo-totalitarianism'. In his view Russia's corrupt system could not exist without the offshore arrangements and support provided by the financial centres of the West.

The cyber guerrilla war started in earnest in 2026 with a series of bombings, assassinations and information leaks primarily targeting the Russian elite and export industries but also Western investment banks and big Western companies operating in Russia – the guerrilla terrorists called them "accomplices feeding the hydra". Some of the bombs were planted in the county's critical infrastructure sites and export facilities. One of the bombs exploded in Rublyovka – an affluent suburb near Moscow where wealthy and powerful Russians live. The attacks often used methods that the Russian authorities had previously directly or indirectly approved to be used against the country's enemies: sarin gas (allegedly stolen from reserves in Syria) and poisonings, for instance. The attacks were backed by information leaks of earlier Russian practices of the same sort – this sent a message that the guerrilla terrorists were not doing anything that the Russian authorities had not already done before.

The Putinist authorities reacted as expected: they launched an aggressive campaign to discredit the guerrillas and to root them out, as well as those who supported them, whether actively or passively. Russia received significant help from China in particular. Many Western governments also cooperated with the Russian authorities – and were strongly criticised for this, leading to deep divisions and rancour within their own societies. Most Russians distrusted both the authorities and the guerrillas; they felt themselves unprotected and on their own just as people had done after the Soviet Union collapsed in the early 1990s. Putin's regime had long been unpopular and the revelations about its operations and practices eroded the little that was left of its credibility. The actions of both the government and the guerrillas had led to the deaths of innocent people, dismissed as collateral damage.

...

Even before the start of Kropotkin's guerrilla war, the Russian economy had been heading towards a catastrophe, and the turmoil caused by the guerrillas proved to be the last straw that broke the back of Putin's Russia. This happened unexpectedly quickly. The irony was that over-investment in state security and the military had made the country economically so weak that around 500-1,000 guerrilla terrorists could bring the whole system down. After 40 years of the post-Soviet experiment, Russia was politically adrift again without a clear political direction or a leader.

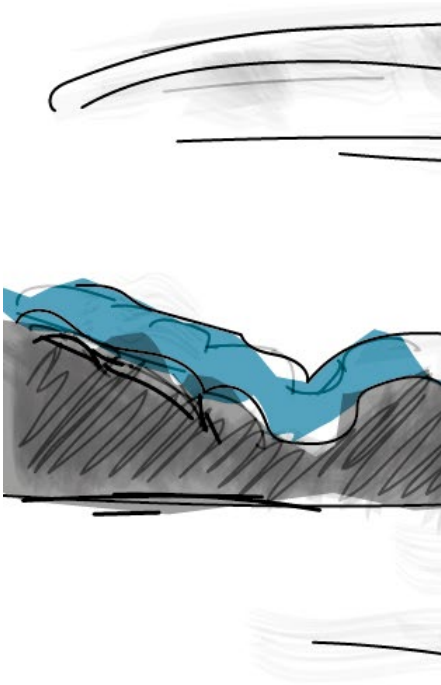
Before collapsing in 2031, the regime managed to eliminate both Andrei aka Kropotkin and Ilya. Kropotkin was killed in Singapore by Chinese special forces on 14 August 2030, and around two months after his death, Ilya allegedly committed suicide in the suburbs of Vladikavkaz. Some of their followers continued the guerrilla fight but the 'Kropotkin movement' was much reduced in size and in its level of ambition. Putin served until the end of 2030 after which his handpicked successor failed to win in the presidential elections. Not even massive fraud could hide the fact that in reality he had no support whatsoever among the citizens. Riots and protests ensued, and a communist candidate was declared to be the president. After just a year and a half in power the communist president was ousted due to malpractice and corruption, and new elections were set to be held June 2033.

THE BIG FIGHT: THE RETURN OF CONVENTIONAL WAR

The big fight: the return of conventional war

No reflection on the future of conflict would be complete without including what we call the conventional war: the open fight between two or more states. In purely numerical terms, this is a rare affair, and has become even rarer since the 1990s. Its comparative rarity has given rise to hope among some that it might disappear altogether.[1] But for the purpose of analysis, rarity means primarily fewer data and insights, and therefore less predictability. The fact that two major wars are never alike does not make anticipation any easier. This means that we still have a very poor understanding of the cause, trajectory and cost of intrastate conflict. This is worrying because when states do go to war, they have the resources and centralised decision-making that make conflicts particularly lethal and destructive. It is perhaps because of this rather anxiety-inducing insight that most of future war fiction focuses on this type of conflict. World War III alone has inspired more than 50 books, including famous ones such as *On the Beach* (1957), *The Third World War: The Untold Story* (1982), *Team Yankee* (1987), or, more recently, *Rescind Order* (2020).

The scenarios in this section reflect on this type of conflict. They portray a future that expresses perhaps 2020 more than 2030: one where states challenge each other openly and violently, using new and old methods, and causing great harm and loss of life.



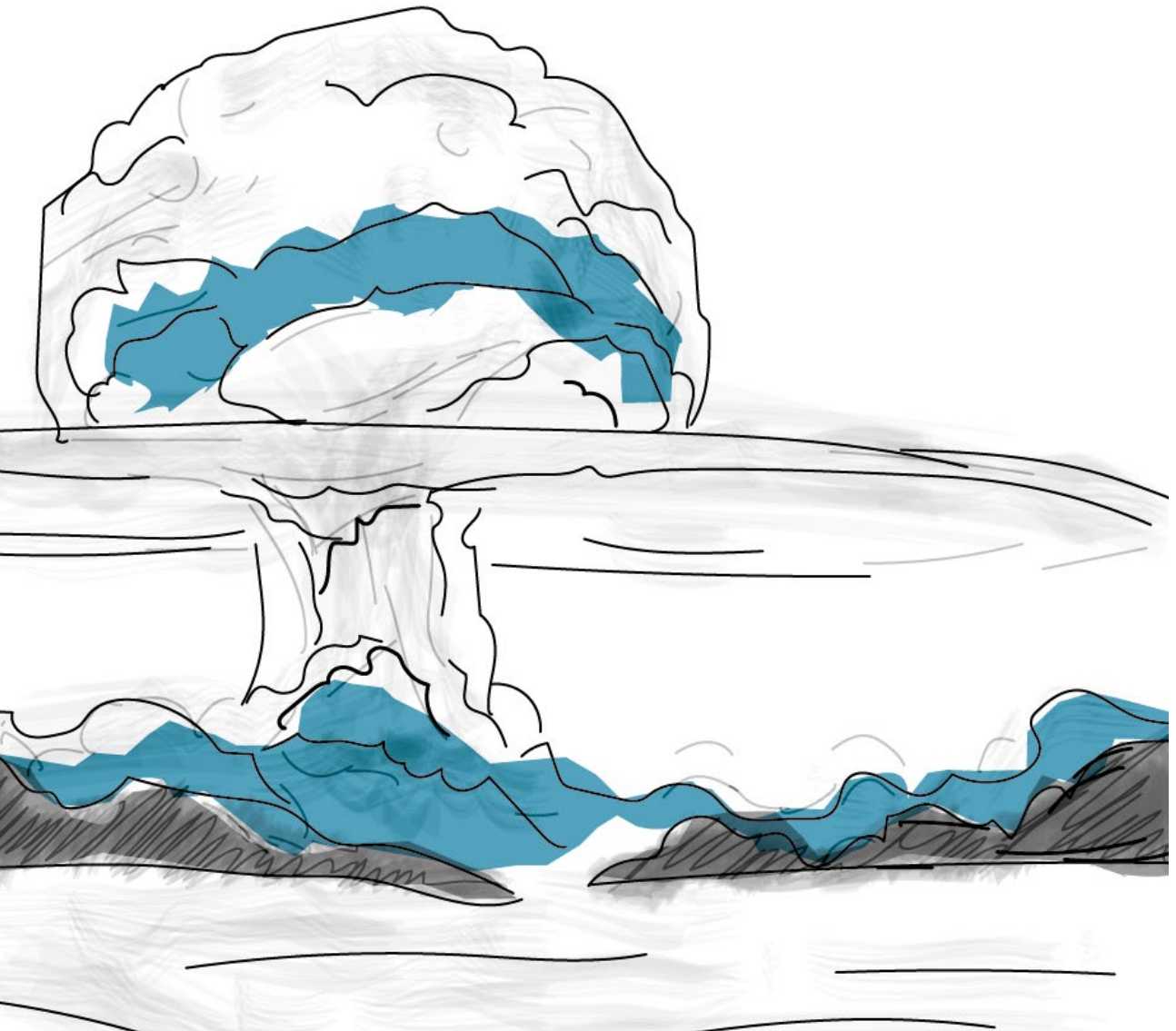
1 Louis J. Halle, "Does War Have a Future?", *Foreign Affairs*, vol. 52, no. 1, October 1973, pp. 20–34.

CHAPTER 6

AT LONG LAST

The US-Russian war

by
ANDREW MONAGHAN



Assumptions 2030

- > Great power competition intensifies
- > Cyber conflicts are no longer confined to the cyber domain
- > Russian-Chinese relations become even stronger

Colonel General Vasily Valerievich Pobedonosny, commanding officer of the Western Military District, thought that the war was in danger of becoming a 'sidyachaya voina': there was too much sitting around, not enough movement in this all-important initial period of the war for his taste. True, the foreign ministry, stung by the disaster that had befallen their colleagues, had already gained considerable – even quite unexpected – successes, securing the neutrality of some states and even winning the active support of others.

Likewise, military preparations were in hand. Kaliningrad was already reinforced to absorb what Pobedonosny anticipated would be powerful blows. Minelaying and other preparations for the defence of the Baltic Sea ports and the Barents Sea were nearing completion, and 'Garmoniya' and the networks of detection and fortifications protecting Russia's interests in the Arctic and along the Northern Sea Route were fully alert. Nevertheless, the pause after the early successes felt to him like a loss of momentum: he feared that the early initiative that Russia had gained was seeping away.

...

Russia's relationship with the US has long been fraught, Pobedonosny reflected. After a difficult few years in the late 2010s, the US had recovered its vigour and direction in the 2020s, retaining its dominance in international affairs. For the last five years, the news headlines have been full of our persistent disagreements. Washington claims that our activity in the Southern Ocean undermines the spirit of the Antarctic Treaty System, and that our Northern Sea Route strategy interferes with freedom of navigation. And we continue to oppose Washington's efforts both to act as a global policeman, and to implement its prompt global strike and missile defence programmes. Only a handful of journalists still recall the major disputes over Russia establishing a presence in Libya in 2021, let alone events in Ukraine in 2014, but Pobedonosny knew that these episodes and their consequences still rankle officials on both sides. The collision of two US and Russian warships in the Baltic Sea in June 2028 had brought us to the brink, from which both sides stepped back, shocked, at the last minute.

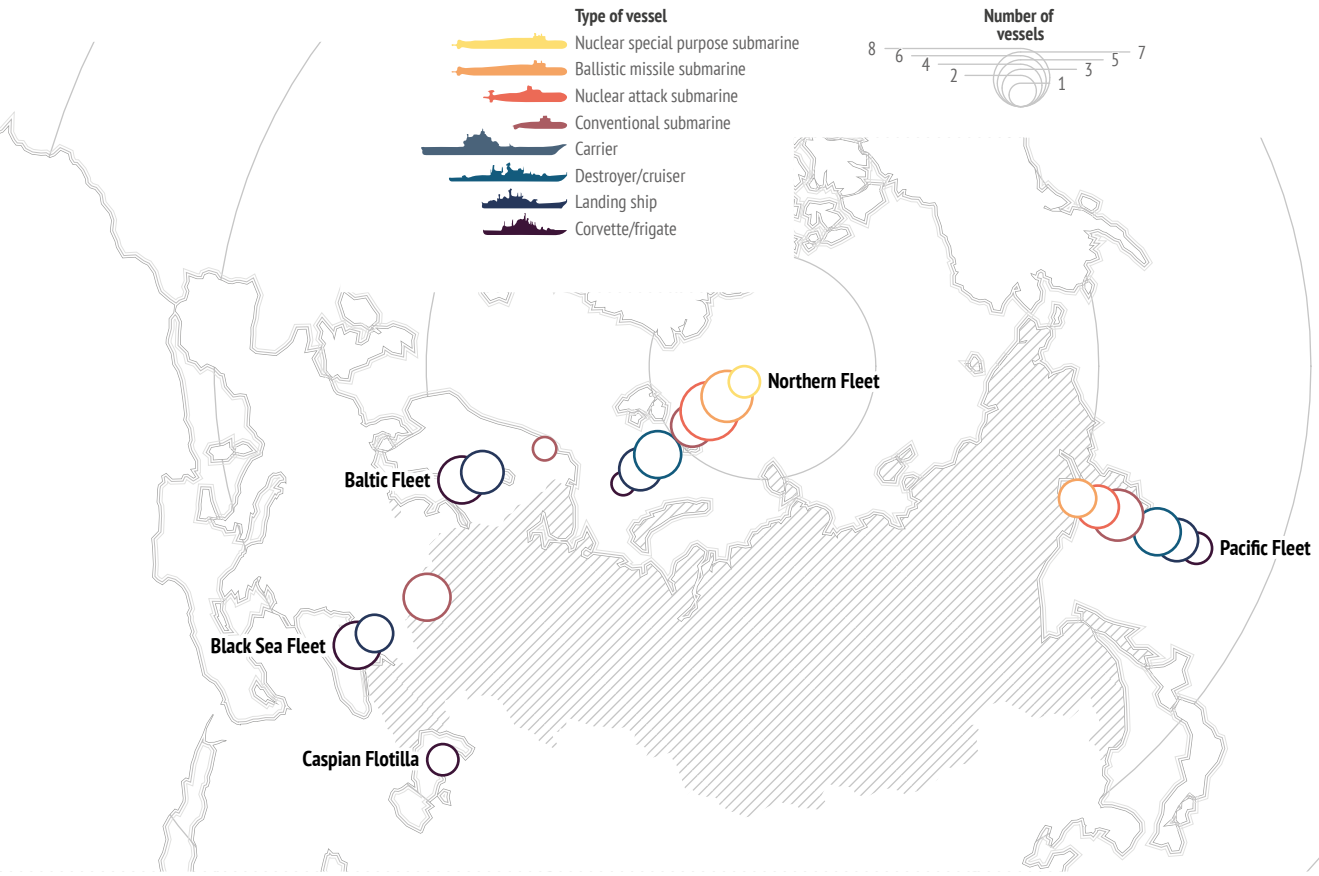
The proximate cause of the war, though, happened four months ago in the Gulf, in late October 2029. The kidnapping of our diplomatic team amid violent street protests and their insulting treatment was provocation enough. But the grotesque public murder of Ambassador Alexander Ivanovich Rubatsky gave Moscow no option but to deploy special forces teams, supported by drone strikes, to free the remaining hostages and punish the culprits.

The many relationships that we had fostered in the region since the early 2010s meant that we knew who was responsible – and who had supported and encouraged them. We did what was necessary: our diplomats were freed, the bandits liquidated. Yet Washington claimed that "once again" we had "showed aggression" and used "disproportionate force" in bringing the perpetrators to justice. Their new president, only a few months in office, was carried away by the clamour in Washington that our activities had now "crossed a red line" and for the US to act to "protect the international order".

Amid the habitual propaganda storm against us came cyberattacks on both our Southern Unified Command headquarters and Situation Centres in western Russia, and also cruise missile strikes on our naval facility at Tartus (from where our rescue mission had been launched) from US ships in the Mediterranean and Red Seas and their aircraft based in the Gulf. Then the American president issued an ultimatum demanding that, among other things, our president resign: they demanded our surrender! Naturally, we immediately "returned the puck to them", as we say. Our president rejected Washington's demands during

Russia's maritime posture

First- and second-rank surface combatants and submarines



Data: FOI, 2019

his annual speech to the Federal Assembly, brought forward to November because of the crisis. "Throughout history", he said, "many have tried to put Russia on her knees and to frighten her – but nobody has ever succeeded". A day later, one of our P-650 special operations submarines sank the USS *Donald Cook* in Portsmouth harbour. Events then moved apace.

Errors were made. That Captain who had – against explicit orders – engaged in a pointless demonstration of strength with the two NATO vessels in Gdansk Bay and hit a mine while returning to port, was a fool. The loss of one of the fleet's old 'self-sinkers' was no loss to our fighting power, Pobedonosny thought, but it was unnecessary – and a propaganda gift to our enemies.

Fortunately, however, the Americans and British acted as our planners had anticipated. A brief gap opened as US forces attempted to redeploy from their extensive commitments across the world, meaning that they had to rely initially on their allies. Thus, the British began to implement the plan they had rehearsed several times during the 2020s to deploy major strike forces to the Pacific Ocean.

This brought Vits-Admiral Fyodor Fyodorovich Ivantsov's visionary preparation into perspective. He had overseen the slow – and thus to many imperceptible – development of our "permanent exercising" across the Indian Ocean: in the Arabian and Andaman Seas, and off Southern Africa. This had enhanced our forward deployed capability, and improved coordination among our own services, Pobedonosny acknowledged, and also built a wider

range of relationships with partners and allies across the region.

Thus, we were able to inflict three major setbacks on the allies in December. On 4 December, our partners in the Yemeni militia, with our advisors and material support, and with submarine support from our navy, conducted Yakhont and Bolid missile strikes on Allied shipping as it deployed to reinforce their units in the Persian Gulf. Surprise was complete. HMS *Albion* was sunk off Al Mukalla, with the loss of many of the 700 Royal Marines and crew. The Ukrainian corvette *Volodymyr Velykyi*, attached to the EUNAVFOR *Atalanta* naval operation, attempted to engage our force but was also sunk. Other rewards would soon be reaped, as Ivantsov had envisaged.

Then, on 10 December, our forces attacked the British carrier strike group deploying to the Pacific. We had located them south of Sri Lanka and struck as they turned towards the Cocos Islands. We deployed long-range aviation and escorts from bases at Malang and Pekanbaru. These were to coordinate with our substantial surface and submarine assets in the area, including the *Dvina*, the first of our Laika Class vessels, and two of our Yasen class boats, to ambush and overwhelm the ships.

Surprise was not achieved, however, and by all accounts the British defence was skilled, sustained and courageous. But our sailors and pilots were aware of the strategic implications of the operation and pressed home the attack regardless. The cost was high. All but one of the long-range aircraft were shot down, along with most of the escorts, and the Kilo-class submarine *Alrosa* and three surface vessels, including the *Gromkiy* and the *Provorny*, were sunk. Captain 1st Rank Alexander Borisovich Tsvetkov, the officer commanding the operation, who closed to engage the enemy with gunfire to ensure success, was posthumously awarded the distinction of Hero of Russia.

But our goal was achieved: the strike group was disrupted. Our forces sank the Type 26 and Type 23 frigates, HMS *Cardiff* and HMS *Sutherland*, and a support vessel. The *Prince of Wales* and two of its escorts, the Type 45 destroyer HMS *Duncan*, and the Type 31 frigate HMS *Encounter*, managed to escape, though all were seriously damaged. They sought shelter in Australia and will long be out of action.

Coinciding with their arrival in Australia, Ivantsov's plan reaped its second harvest. The aggressive convoying that the Allies imposed after HMS *Albion* was lost resulted in the harassment and boarding of an Iranian vessel, and then, two days later, the firing of warning shots at the PLAN destroyer *Guiyang*. In the sharp engagement that followed, 38 Chinese sailors were killed. These engagements leave us astride the main trade routes of the Indian Ocean, and the way the Allies have reacted has caused a swarm of activity hostile to them around the Horn of Africa and beyond.

But it was the similar engagement in the Central Mediterranean that secured the initiative for us. Our regional alliances with Libya and Algeria had extended our permanent presence into the Central Mediterranean by 2022. Our forces there had slowly grown in strength, and on 17 December, our Central Mediterranean flotilla, with air support from bases in Libya, fought an encounter battle with a NATO force that sought to reopen the route to the Indian Ocean. Again, we suffered heavy losses. But again, the superior firepower our ships brought to bear in the artillery battle – especially from Admiral Amelko and Admiral Essen – dispersed the NATO force with substantial casualties, including the sinking of two of the American vessels that had taken part in the strikes on Tartus.

...

Our active defence ensured that the Allies' attempts first to move into position and then to relieve their parlous situation have been neutralised. Their reliance on exquisite capabilities and technology came at the cost of available numbers, and thus presence and resilience. Their recognition of the value of numbers came too late: force regeneration will take time. The value of concentrated firepower in war was also again demonstrated. Our losses at sea are not insignificant; but replacements are already deploying; and the navy's initial task has been

fulfilled. Our submarines now patrol the Atlantic and Pacific.

The geopolitical tide has conclusively turned. Washington's main ally has endured a severe blow, and NATO is in shock having suffered its first real defeat in battle. Their reactions have worsened their own position. With Iran on our side, we harry remaining Allied forces in the Persian Gulf from all sides. And with China on a war footing and mobilising its forces, the US faces a worldwide multidimensional challenge.

Washington is well aware of our escalation capabilities. We have shown that we respond to a threat by creating a threat. Whether this evolves from being a regional war to a large-scale war is their choice; they will surely realise the futility of continuing. Our president has stated that any further move against us will result in our full mobilisation and deployment of strategic forces, including nuclear capabilities. It will be a defensive war for us: we have resilience in system, numbers and spirit. Nearly 20 years ago, Valery Vasilievich Gerasimov announced our intention to be materially prepared with everything necessary in the appropriate quantity before the outbreak of any war, and subsequent State Armaments Programmes have ensured that.

So, Pobedonosny thought, European leaders find themselves in a difficult position, and the implications are now looming large. Their economies already face a dramatic situation. Oil prices, rising since November, have just hit $200 a barrel. The 'Global Connectivity' plan with Asia on which the EU's economy has become so dependent – more than 94% of their trade with Asia is seaborne, mostly through the Indian Ocean – is now *de*-connected. The EU's internal debate about engaging in the extended neighbourhood is now fractious and angry. In this short pause in the fighting, our diplomats offer them a choice: stay neutral and commit to reconnecting with Asia via the much shorter Northern Sea Route at favourable transit rates, or join the Americans and face economic blockade and military bombardment.

CHAPTER 7

GLOBO-COP'S LAST FIGHT

China and the US clash in Africa

by
KATHLEEN J. MCINNIS

Assumptions 2030

- > Domestic fragility undermines US military preparedness
- > The US and Europe rekindle their relationship
- > European military capabilities are no match for Chinese
- > China is ready for and capable of undertaking offensive war
- > Other states bandwagon on the conflict

UNCLASSIFIED

ANNEX 3A: TESTIMONY FROM KEY US OFFICIALS

INTERVIEW WITH SUSAN DACEY, WHITE HOUSE CHIEF OF STAFF, PRESIDENT LUKE HAGEY ADMINISTRATION

SUSAN DACEY: It's still amazing to me how the basic 'facts' of what happened over the past five years are actually just plain wrong. A lot of folks call it the third world war, for example, but I think that's lazy. It's more like a global free-for-all triggered by the mess that started in the US. Of course, there's a lot of people who want to blame this on Lieutenant Colonel Mayberry, but that's lazy too. The world had become a powder keg well before he decided he knew better than his bosses what to do out there in Djibouti.

Then again, everyone – and I mean everyone – has had their PR machines spinning; most people could be forgiven for thinking that white was black. Anyway, I'm really glad this Commission was set up, and glad to be talking to you.

COMMISSIONER: We appreciate your time.

DACEY: There's so much misinformation out there... In order to tell the story, I think it's best to go back to the beginning.

COMMISSIONER: Sure. However you want to proceed.

DACEY: Let's see. In 2027, I was Governor Hagey's Chief of Staff. When he got elected, I was pulled into the White House, where I served as his Chief of Staff again. I was in the West Wing when we got the news about Djibouti. 25 March, 2030. I'll never forget that day.

COMMISSIONER: Go on.

DACEY: We were in the middle of refining the Settlement of the States. Remember when that was the most pressing issue? Whether we could avoid another US civil war? It feels like ancient history. Anyway, we were thrashing out the details of the new Constitutional amendment to rebalance on state versus federal government agencies. The 2020 pandemic exposed the cracks, of course, but frustration in the states had been brewing for a long time before that. In 2020, what started as frustration that the Feds hadn't stockpiled essential supplies turned into outright anger that the few meagre supplies they did maintain were withheld. Governors in different regions quietly worked with each other in regional clusters to solve the problems. We muddled through. But the cracks turned into canyons in 2026 when the Feds raised taxes – during the recession! – and *still* didn't stockpile essential supplies. They spent it on that crackpot military plane that turned out to be useless and Wall Street bailouts.

In late 2028, we *should* have been prepared for the swine flu. But the Feds blew it, again. That was what opened Pandora's box. Everything that had been festering for years: abortion rights, anti-vaxxers, racial divides, gun control... all of it was out in the open and everyone was angry. I hear from my counterparts in Europe that a number of national capitals were feeling similarly frustrated with the EU, so our key allies had their hands full with domestic crises too.

COMMISSIONER: How did you hear about the incident in Djibouti?

DACEY: We'd just about gotten to a solution that everyone could agree with. I was sitting with the States' representatives and Congressional leadership hammering through the compromise when my Deputy, Bill Greely, passed me

a note and said I was needed in the Situation Room. When I got there, all we knew was that Chinese and American forces were in a firefight with each other in Djibouti, and that there were casualties.

For years, we put our military on a pedestal. We liked to think that our military is above reproach. But it turns out that some nasty, white supremacist elements had risen in the ranks and felt they knew more than anyone else. Of course, Mayberry was a Fed guy. Turns out he thought Hagey was a traitor. The experts call this kind of stuff 'civ-mil relations', and we'd definitely reached a low point. Mayberry decided he didn't recognise his chain of command anymore because Hagey was "not a legal President." Anyway, he decided to take matters into his own hands when it came to Chinese harassment.

COMMISSIONER: Harassment?

DACEY: It's amazing, how much damage one little thing can do. All that damage, all those lives lost, because of a laser pointer. A Chinese soldier pointed it at the windshield of a C-17 with some of Mayberry's men on it. There was a bunch of other stuff that went wrong with the instrumentation that night – you can read the reports - but the bottom line is that when it crashed, Mayberry lost twenty of his men. He decided to take matters into his own hands.

A war that spanned the world, all because of a laser pointer and a Lieutenant Colonel with an overweening sense of entitlement.

(Inaudible)

Of course, China wasn't interested in our explanation that Mayberry had gone rogue. They'd reached the point where they thought they could do anything, take on anything. Years of propaganda and concentration of power under Xi Jinping meant they were spoiling for a *big* fight. And all the chaos in the United States made them feel that the time was right; they calculated that the US wouldn't be interested in playing Globo-cop anymore. Looking back, they weren't completely wrong.

COMMISSIONER: Most people are of the view that this was a war between the US and China. Why do you say it was *(shuffling of paper)* a 'free for all?'

DACEY: Because it *was*. Different countries joined the fray, picking a side, more to settle their own scores. Take Pakistan. Sure, it sided with China. But that was a pretext for its attempt to annex Kashmir. Millions died in that 'limited' nuclear war, as the experts called it at the time. *(Pause)*. I was at a dinner with a Yale historian the other night, who pointed out that this was the first global conflict of the post-colonial era.

COMMISSIONER: Meaning?

DACEY: Meaning that it wasn't the political objectives of a handful of empires crashing into each other; it was the political objectives of *dozens* of states. Iran taking Iraq. Armenia and Azerbaijan. Russia annexing the Svalbard Islands. Yes, they'd ostensibly chosen China's side. But from where I sat, our fight with China was more pretext than anything else.

COMMISSIONER: What do you say to the criticism that the US could have done more?

DACEY: Yeah, that's a favourite dog whistle these days; if the US had been more aggressive and robust at the outset, it would have prevented the conflict from going global. Escalate to de-escalate, they say. Maybe that's true, but I personally don't see how. We've had our hands full managing our own domestic situation – preventing a civil war – and there are a lot of states who were, and are, happy to just let the world deal with itself. So, our ability to respond has been politically limited. Making matters worse, our closest allies were hobbled right from the start, so building a collective response was pretty tough.

COMMISSIONER: You're referring to Europe?

DACEY: Yes, although Japan was in pretty dire straits too. Everyone was. After the Chinese bombed out US bases in South Korea, Guam and Japan – effectively cratering our posture in the region in one attack – our allies became sitting

ducks, especially after the Chinese navy deployed undersea drones to prevent our navy's access to the region. And because China had disabled our satellites and telecommunications networks, there was little we could do about it. It would be a while before we could send reinforcements, so the Chinese decided to change the facts on the ground by eliminating the US-footprint in Asia.

Europe... well, Europe got sucked in because China wanted to use their Belt and Road infrastructure for the war effort, and to their credit, most of our allies declined. Malta and Hungary siding with China, though – I guess that was probably the death knell of the European Union and NATO. Anyway, Europe felt the economic squeeze, hard. Years of Chinese cash floating around their economies was suddenly shut off. I remember seeing that Europe hit 55% unemployment at one time. *Fifty-five percent*. That's around two hundred and sixty million people. War mobilisation has helped with that.

Ironically, it hasn't been quite as bad in the United States because of the devolution of power to the states, but it's not been great, either. We're hovering at 35%. And Europe's military capabilities? Well, they're able to mount a pretty decent territorial defence, but that's not how China is playing the game. If they were able to bring the fight to Asia – if we could mount a collective response there – that would be one thing. But they can't.

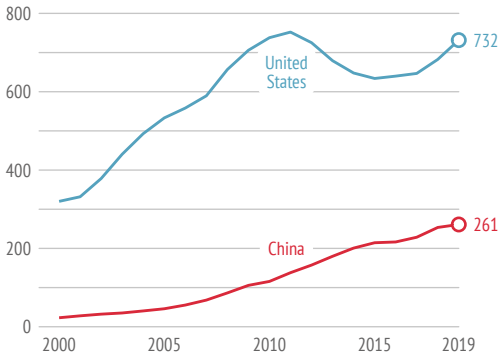
As for now, well, it's going to be a hell of a slog. All that Chinese intellectual property theft? Acquisition of companies with key technologies? Yeah, those chickens came home to roost. The tech that was initially designed by Kuka robotics has been used to manufacture advanced Chinese artillery and ballistic missiles. The ones used against our bases in Asia. The plan is to retake our positions, but as you know it's been a massive R&D effort to develop the capabilities we need to begin re-establishing ourselves there.

(Pauses)

My Department of Defense colleagues see naval and air assets being the primary means of

Chinese and US military spending

2000–2019, current $ billion (converted at the exchange rate for the given year)



NB: Figures for China are SIPRI estimates. Data: SIPRI, 2020

retaking our positions in allied territories, as they will help us break the A2/AD 'bubble' that China has built, both underwater and in the sky. Their innovations on the AI front have been tough to match, operationally. They're faster, probably because they didn't care as much as we did about keeping humans 'in the loop' with unmanned drones. Don't really care about civilian casualties either, for that matter. We're trying to figure out how to find a weakness there and exploit it. And their logistics and resupply capabilities aren't the best, either. The DOD folks keep thinking about how to re-establish technological superiority, but I keep wondering if more low-tech, cheaper solutions would be better. Cheap swarm drones, stuff like that. Grind them down. Regardless, all the answers for dealing with mainland China seem pretty grim right now.

Can I raise something that's been on my mind?

COMMISSIONER: Sure.

DACEY: The death toll. It has been staggering.

COMMISSIONER: Yes, it has.

DACEY: Yes, but it's going to be a long time before we have the real numbers. There's the official count of military deaths, which has been in the hundreds of thousands. But then there's the 'ethnic cleansing' in China and India, and

Turkey's annexation of northern Iraq and Kurdistan, hundreds of thousands – millions – have died. Then there's the disruption of food supply chains and the ripple effects of the recession across the globe. We were worried about the numbers from the nuclear parts of this war, but I'm much more worried about the casualties caused by the opportunism and economic collateral damage. I don't know when this war will be over, but it'll be much harder to recover if we don't have enough *people* left at the end of it. And, for that matter, how does this end? There are so many parties to the conflict, with so many different agendas, how do we find peace?

END ON-RECORD INTERVIEW.

##

CHAPTER 8

THE VIBER INVASION

How Russia occupied Montenegro

by
FRANZ-STEFAN GADY

Assumptions 2030

- > Intelligence operations merge with disinformation campaigns
- > Russian Special Forces spearhead a territorial occupation
- > European military capabilities and political will do not extend to the Balkans

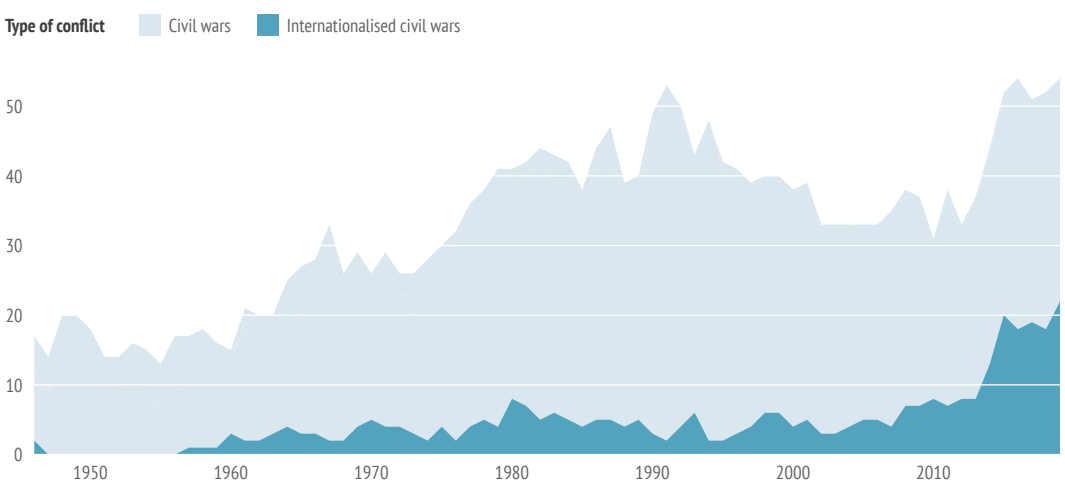
Special alert: "US Servicemen Gang Rape Montenegrin Woman and Desecrate Church in Booze-filled Night Out."

Over 10,000 inhabitants of the capital of Montenegro, Podgorica, wake up to the same push notification headline on their Viper instant message app. Each target has received the message from the user account they had most interacted with on the messaging app over the previous five days and each message is slightly different. When the recipients click on a link, they find a four-minute-long iPhone 16 video clip showing three English-speaking males, identified via facial recognition software as Americans, ostensibly assaulting a young Montenegrin woman in a dimly lit room. The laughs of the men and the cries of the woman begging them to stop are clearly discernible. After two minutes of graphic footage, the video cuts to the same three men in front of the Cathedral of the Resurrection of Christ. The video identifies the time as 5 a.m., 12 August 2030: two of the Americans are seen urinating against the wooden church door while laughing, their slurred speech barely intelligible.

This is just the opening salvo of the Russian campaign of AI-enabled automated disinformation strikes. As the video organically spreads through the Montenegrin population, thousands of AI-chat bots begin inundating the social media accounts of journalists at the *Vijesti* and *Dan* newspapers, as well as the public service broadcaster *RTCG*. A select group of Montenegrin politicians are receiving the video seemingly from analysts at the country's National Security Agency, with the shocking revelation that one of the Americans in the video is the head of the Office of Defense Cooperation at the US Embassy in Podgorica, another a member of a joint US-Montenegrin cyber defence unit, stationed at the armed forces headquarters in the capital. Russia had infiltrated the unit three years ago, when Serbian military intelligence recruited a young Montenegrin of Serbian descent, whose father was killed in the NATO air campaign against Serbia in 1999. Russian operatives and pro-Russian elements in Serbian military intelligence are fed intelligence from their spy about the individual

Civil conflicts by international involvement

An internal conflict is regarded as internationalised if one or more third party governments are involved with combat personnel in support of the objective of either side. 1989–2019



Data: UCDP/PRIO Armed Conflict Database, 2020

Americans in the joint cyber defence unit with whom he had become very friendly. It was his iPhone a year ago that recorded the video of the three Americans' night out.

It was at his behest that they went to a house party and passed the church. However, the rape and urination never happened. Russian synthetic media specialists carefully created the now viral video by applying machine learning methods and generating deepfakes of the three men and the woman, who was digitally simulated. The US embassy and cyber defence unit were quick to point out that the videos were fake, but their argument was immediately dismissed as damage control.

Within hours, protestors, led by clerics of the Serbian Orthodox Church, are gathering in front of the US Embassy in Podgorica demanding the immediate extradition of the three suspects and a public apology from the US president, Tom Cotton, a Republican and fierce nationalist, who had just assumed the presidency in January. He had been quoted during his election campaign as saying that "the whole of the Balkans is not worth the blood of a single American Marine" and repeatedly calling into question US defence commitments to Asian and European allies. Montenegro had only joined NATO in 2017 as its 28th member. Its armed forces consisted of 2,000 lightly armed troops, a small fleet of vessels, a few dozen armoured vehicles, and a number of old aircraft.

The crowd of protestors in front of the embassy had been infiltrated by members of Unit 29155, an arm of Russia's military intelligence agency, GRU, who flew into the country as Russian tourists under the visa-free travel pact between the two countries. The protests, led by GRU. agitators, and fuelled by genuine public anger, quickly turn violent. As local security forces are brushed aside, President Cotton, haunted by the 2011 attacks on US government facilities in Benghazi, had ordered the Marine detachment guarding the embassy to defend the compound with lethal force if necessary. The Marines shoot and kill a Russian GRU operative brandishing a gun. The crowd quickly disperses. Minutes later, canned social media alerts report that a US Marine killed a Serbian-Orthodox cleric, leading to a public outcry not only in Montenegro, but also in Serbia and Russia.

...

An independent analysis of the material by an international collective of researchers and investigators pointing to the fabrication of the material fails to mitigate public anger.

The Montenegrin pro-Western government, headed by a politician of the long-ruling Democratic Party of Socialists of Montenegro, is split between a faction demanding an immediate breakoff of diplomatic relations with the United States unless the suspects are handed over and a group advocating for a more nuanced approach and independent investigation of the events. President Cotton makes it clear that he does not accept Montenegrin jurisdiction over two of the three soldiers accused (the head of the Office of Defense Cooperation carries a diplomatic passport), repeatedly calling the videos and accusations "fake news." Various Russian-sponsored news outlets are now incessantly also reporting about a supposed secret deal brokered by the United States and endorsed by the European Union to promote the eventual establishment of a Greater Albania, comprising territories inhabited by Albanians in Montenegro.

Protests are meanwhile spreading across Montenegro, including by the end of August the beach resort towns dotting the coast. The protests are accompanied by mysterious power outages, which Montenegrin authorities claim are due to state-sponsored cyberattacks from an unknown country, but in fact were curated by Russian hackers. AI-enabled chat bots float social media networks with calls for the government to resign as it cannot even keep the state's lights on at night.

Reports of mysterious armed men roaming the Montenegrin countryside are summarily dismissed by the authorities, who do not want to further fuel the spiralling rumour mill.

In fact, in July 300 Russian special operations forces (SOF) from Special Operations Command had flown to Montenegro as 'tourists',

who rented various beach properties at strategic locations along the coast. Four Project 636.3 *Kilo*-class diesel-electric attack submarines of the Russian Black Sea Fleet had delivered weapons and ammunition at night-time to equip this shadowy force. They were supported by elements of the Albanian-Montenegrin mafia, which is rumoured to have close ties to some of the incumbent ministers in Podgorica, and who have a vested interest in replacing the pro-Western government in Podgorica with a pro-Serbian/Russian faction less keen on cooperating with European and US transnational crime fighting authorities.

...

After an explosion blamed on a lack of oversight and corruption (but in fact carried out by Unit 29155) at the Pljevlja power plant, which had only been recently modernised in the early 2020s, public protests reach fever pitch and the incumbent government is forced to resign and replaced by a government headed by the Serb ethno-nationalist Democratic Front. The US embassy meanwhile by the last week of August had evacuated its entire personnel outside the country, including the three suspects, on the direct order of President Cotton. The US-Montenegrin cyber defence unit is dissolved, and its US elements transferred to a military base in Germany. The government's first motion is to announce the country's withdrawal from NATO. It sends the US, as NATO's depository, a "notice of denunciation" with Montenegro officially leaving the alliance by August 2031. Notably, the new government also concedes to a Russian request to dispatch a small force of security personnel to select communities to protect Russian citizens from violent protestors. The outgoing Montenegrin government protests vehemently against this move, as does the EU, and a number of European countries. The head of the dissolved government announces publicly that a Russian military coup is taking place and that Montenegro should invoke Article V against Russia.

Meanwhile, the 300 Russian SOFs along with Montenegrin authorities arrest pro-Western officers in the security branches as well as politicians including the former president. The majority of the Montenegrin public supports these actions, but European authorities and NATO are uncertain how to respond. President Cotton, who had overseen the redeployment of the majority of US forces to the Indo-Pacific region, sees the troubles in Montenegro as a "European" problem. He also does not want to unnecessarily provoke a nuclear power. Germany and France call for an international response to the ongoing crisis but refuse to commit military forces. The NATO Council convenes but cannot commit to military action without the United States.

It is all too late in any case. Throughout August, Russia and Serbia had been conducting a joint military exercise, *Slavic Shield 2025*, on Serbian territory. Over 2,000 Russian airborne troops and an entire battalion of S-400 Triumf air defensc systems, as well as Pantsir-S1 batteries, are participating in the event. The air defence systems were flown in by AN-124 Ruslan transport planes. Only two hours after the new Montenegrin government conceded to the Russian request, Russian transport aircraft land from Serbia carrying the S-400 and Pantsir-S1 batteries, which are immediately deployed at the airport, as well as the first cohort of Russian airborne troops. A Russian TV crew live broadcasts the deployment of the missile batteries repeatedly emphasising that they are armed with the weapon systems' most advanced interceptors – the 40N6. Russian submarines are blocking – or guarding – the country's main naval port at Bar. The Montenegrin government has asked its armed forces to stand down and cooperate with the Russian military. Few resist the order. Two days later, Russian cargo ships bring naval infantry Spetz units into the country.

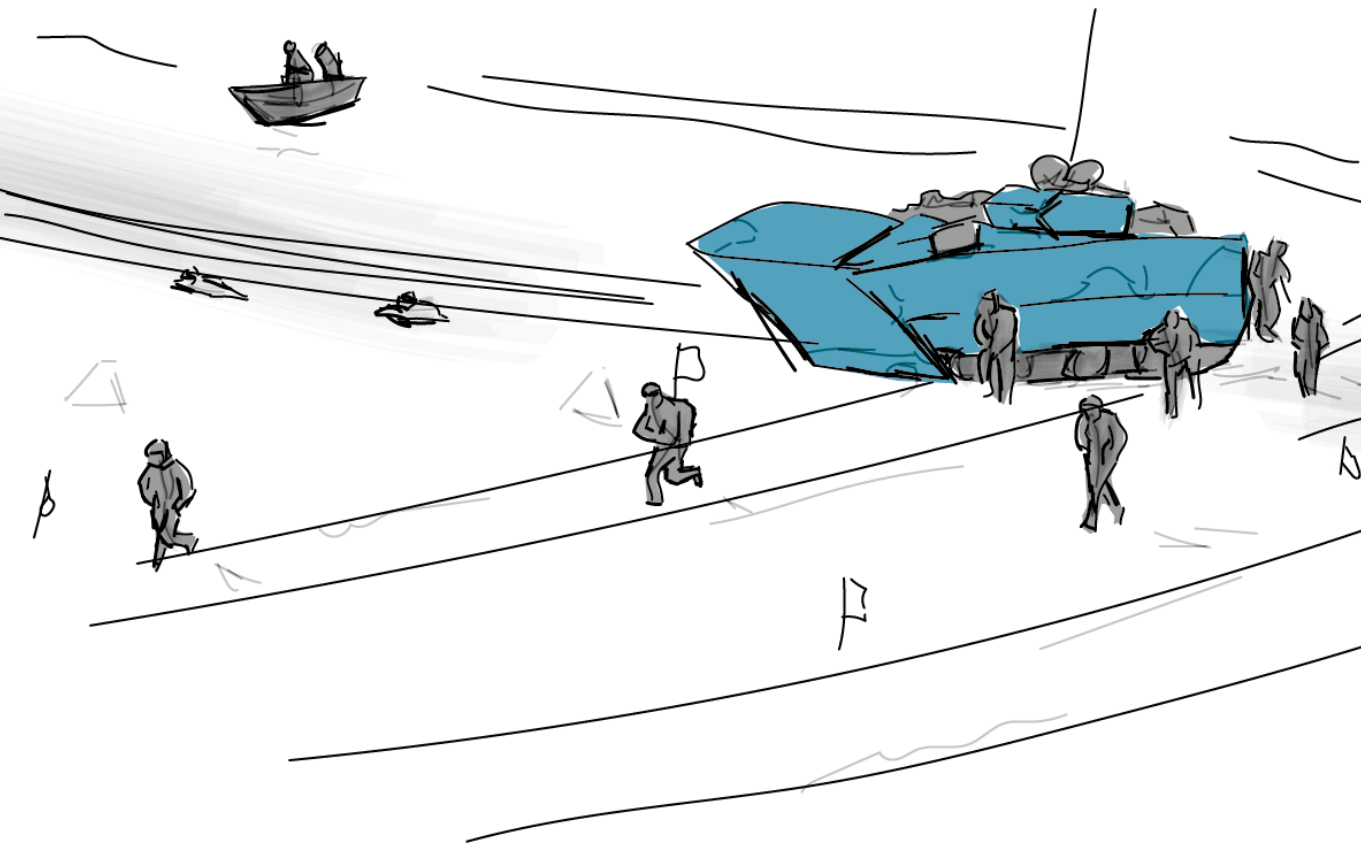
Russia has achieved its military *fait-accompli* in the Western Balkans.

CHAPTER 9

TAIWAN ATTRITION

China crosses the Rubicon

by
BRUNO TERTRAIS



Assumptions 2030

> China reaches a level of military capability allowing for sustained and offensive operations

> The United States continues on its path of retrenchment

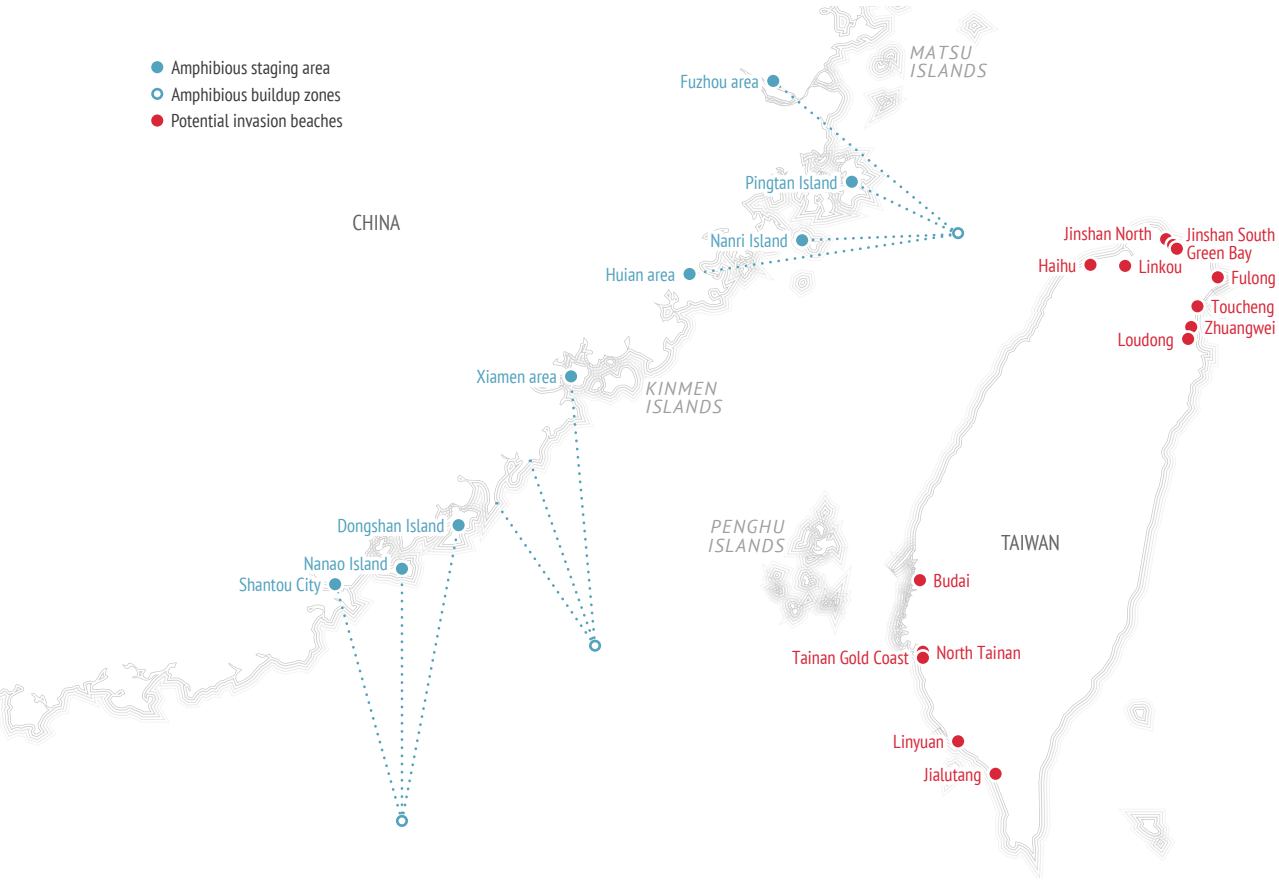
> Deterrence fails

Admiral Qian Lihua looked at the sky from the deck of the *Shandong*, China's newest and flagship aircraft carrier. Even though dawn was now breaking, the dark grey colour of the sky made it barely indistinguishable from the ocean below. Some of my ancestors might have seen this as a bad omen, he thought. But he was confident that this would be one of the most glorious days of the People's Republic. The People's Liberation Army Navy (PLAN) had grown into a formidable force.

For days now, a barrage of several hundreds of ballistic and cruise missiles had saturated the island's defence bubble. Most Taiwanese ports, air bases and unprotected communication centres were rendered unusable. The relentless assault was accompanied by electro-magnetic attacks which crippled Taiwan's ability to defend itself. Only the northern part of Taipei was preserved for fear of accidentally bombing the National Palace Museum, which hosted the most precious Chinese historical artefacts and had been transferred hastily to the island in 1949. A massive cyberattack followed even as underwater cables were cut off.

This was no strategic surprise, and tactical surprise had disappeared the minute the first missile had landed on the island. The People's Liberation Army (PLA) was implementing

Attacking Taiwan by sea



Data: *Foreign Policy*, 2018

its playbook, entitled 'Joint Island Attack Campaign'.

The time had come and the order was given by Beijing. The amphibious assault began in the early hours of the morning. Tens of thousands of highly motivated and trained PLA soldiers loaded with medical stimulants and equipped with 3D goggles giving them real-time access to tactical information on their surroundings landed on the island. The first wave, on a dozen beaches of the west coast, and the ensuing long slog over Taiwan's mudflats, were a bloody carnage for both the invasion force and the civilian population on the heavily populated coast. The landing ships came back to the mainland to bring fresh PLA troops. And they kept arriving, even when their numbers were reduced by Taiwanese mines in the straits and attrition on the battlefield, as airborne commandos parachuted in the rear seized other critical defence and logistical points in the island.

Meanwhile, the PLAN was stopping all Taiwan-bound tankers and ships navigating in the South China Sea.

Two days after the landing, it was clear that the island was resisting, both militarily and socially. But Beijing was in for the long haul. The plan was not to occupy Taiwan but to weaken it enough so that Taipei surrendered.

...

As America licked its wounds after the 2020 pandemic, under the stewardship of a Democratic administration, China became stronger if ever more authoritarian. Meanwhile, in Taiwan, the pro-unification forces got weaker and weaker.

Senator Rand Paul was elected president in November 2028 on an 'American Rebirth' platform. He sought a new grand bargain with China, based on the idea of a 'Free and Open Pacific Ocean'. But China sensed weakness. Toning down its aggressive diplomacy of the 2020s, it embarked on a quieter, humbler charm offensive in the region, based on smart investments in companies, NGOs and currying favour with politicians. The biggest success for Beijing was the patient construction of a *de facto* alliance with Indonesia.

In Zhongnanhai, the debate was raging about what to do with Taipei. The PLA generals insisted that a window of opportunity was opening. US military modernisation had been delayed by the budgetary cuts of the 2020s, but Beijing could perhaps not afford to wait for another decade. Especially with the growing recruitment problem the armed forces were having due to the dramatic fall in birth rates since the beginning of the century. This was now the time to incorporate Taiwan in the Republic, they argued. We will make it another Hong Kong, and then fully integrate it by 2049. The Americans will not have the stomach for a fight and some of their allies, like Thailand and the Philippines, are now outside their sphere of influence. It is maybe now or never. President Li was hesitant. He had been elected just one year before, following Xi Jinping's sudden death, and his power was less assured than his predecessor's. Consensus was important. "We will wait for the right moment", he said.

They did not have to wait for long. President Paul had agreed to support some of the candidates running for Congress at the November elections. One evening in September, he was asked by a crippled veteran of the 2026 Great Persian Gulf war whether he could ask Americans to die for Taipei. That evening, he was exhausted by a mild illness he had suffered the week before and reportedly preoccupied by family problems. While he did not realise it, his reply would earn its place in the history books: "*Actually, I'm not sure that the fate of one little island is a truly vital interest of the United States... I mean... Of course America would defend itself and its allies against any aggression but... What I mean is... I don't want to send our sons and daughters to fight in distant parts of the world just because of the tantrum of some local president... That's not what I was elected for".* Historians warned that this could go down in history as the equivalent of Secretary of State Dean Acheson's 1950 speech in which he explained that the Korean peninsula was not part of the US "defensive perimeter" – which was interpreted as a *nihil obstat* for the invasion of the South.

They were right. The decision was made to attack the island after the October 4 anniversary celebration, taking advantage of the movements of troops needed for this year's massive parade. October was also a good month weather-wise, with a limited chance of heavy storms.

Beijing did not have to worry too much about the other actors in the region. South Korea was too busy with the North, and Russia would obviously remain neutral. The most important parameter was the attitude of Japan. Here China played its hand cleverly. In late September, emissaries of Beijing secretly went to Tokyo to propose a groundbreaking deal: the People's Republic of China (PRC) would publicly acknowledge Japan's sovereignty on the Senkaku/Diaoyu islands provided that Tokyo gave private assurances it would not interfere in a conflict over Taiwan – and forbid the use of its territory for military purposes by any outside power during such a conflict. An ageing and weakened Japan, which had not yet recovered from the Great Tokyo Earthquake of 2027, agreed.

As Asian markets lost 25% of their value in less than two days, America was hesitant. In the White House, President Paul faced mounting pressure to intervene immediately to restore the credibility of US commitments and alliances. The tipping point came when images appeared in the media of several dozen dead Americans who had been living in Taiwan.

But Pentagon planners were about to face their biggest challenge in decades. The use of Forward Deployed Naval Forces (FDNF) in Japan was now impossible. So they decided on a different strategy: while Guam- and Hawaii-based troops were rushing to the conflict zone, the US Marine Corps would open a new front in the south and attempt to bottle up the PLAN in the South China Sea, as envisioned by the new USMC doctrine of 2020.

Railguns and swarms of armed drones began to destroy PLAN ships, while Marines began 'island-hopping' and destroying Chinese infrastructures built on disputed islands. But this was not an easy task. China managed to activate computer viruses that had been implanted in US command, control and communication systems.

Meanwhile, Europe was panicking. Even though it had reduced its economic and financial ties with China, its financial markets had plunged almost as much as Asian and US ones. As populist forces argued that Europe "should have no dog in this fight", there were pressures from Washington for Europe to "hold the fort" on the continent and increase its naval presence in the Persian Gulf to ensure no other country would take advantage of the situation. A UK- and France-led naval task force was sent to the Malacca and Lombok Straits to ensure freedom of navigation. Beijing warned London and Paris to stay out of the conflict, publicly reminding them that European territory was vulnerable to its intercontinental missiles. In return, London and Paris made a solemn joint statement affirming their willingness to "protect their national and European vital interests by whatever means necessary".

China struck back. It destroyed twenty US satellites in a few hours. On Monday, 29 October, a nuclear weapon exploded in the atmosphere over Hawaii, creating havoc in electronic circuits all over the archipelago. But the Pentagon was ready. As directed by President Paul in case such a scenario happened, US forces began to unleash a storm of firepower on the PLAN. Its bases and forces on the mainland were methodically destroyed, even at the price of significant collateral damage. The Chinese had not anticipated that war would come to their shores. Despite the suppression of social networks, it was becoming clear that the population would not tolerate this. Images of thousands of grief-stricken families lamenting the loss of their loved ones multiplied in the media. The China Dream had turned into a China Nightmare.

...

Under strong pressure from Congress and public opinion, newly-reelected President Paul was driven to adopt a new stance towards Beijing. "*We have no choice but to contain any further expansionism of Chinese power*", he said in his 2031

State of the Union address, "*even if it means that a new bamboo curtain is drawn in Asia*".

The US administration announced a costly and painful five-year plan to become "independent from China" and cut off its access to US financial markets. It terminated the US-Japan and US-Korea alliances.

The electronics industry suffered from the war and had to be completely reorganised. A US-European financial conglomerate was rapidly created to help rebuild national manufacturers of computers, smartphones and semi-conductors.

2031 thus marked the symbolic end of globalisation. Meanwhile, Beijing sought a new strategic partnership with Russia, who had patiently waited on the sidelines. And was now in a much better negotiating position than had been the case earlier in the century.

Taiwan was unconquered but considerably weakened. And now, it was on its own. In Zhongnanghai, options on what to do next were discussed. Should Beijing propose a 'truce' to Taipei? Offer a new 'partnership' with the island? Should it make a new attempt next year? The Central Military Commission arrived at a consensus: Beijing would bide its time, but Taiwan would be fully reunited with China before 2049.

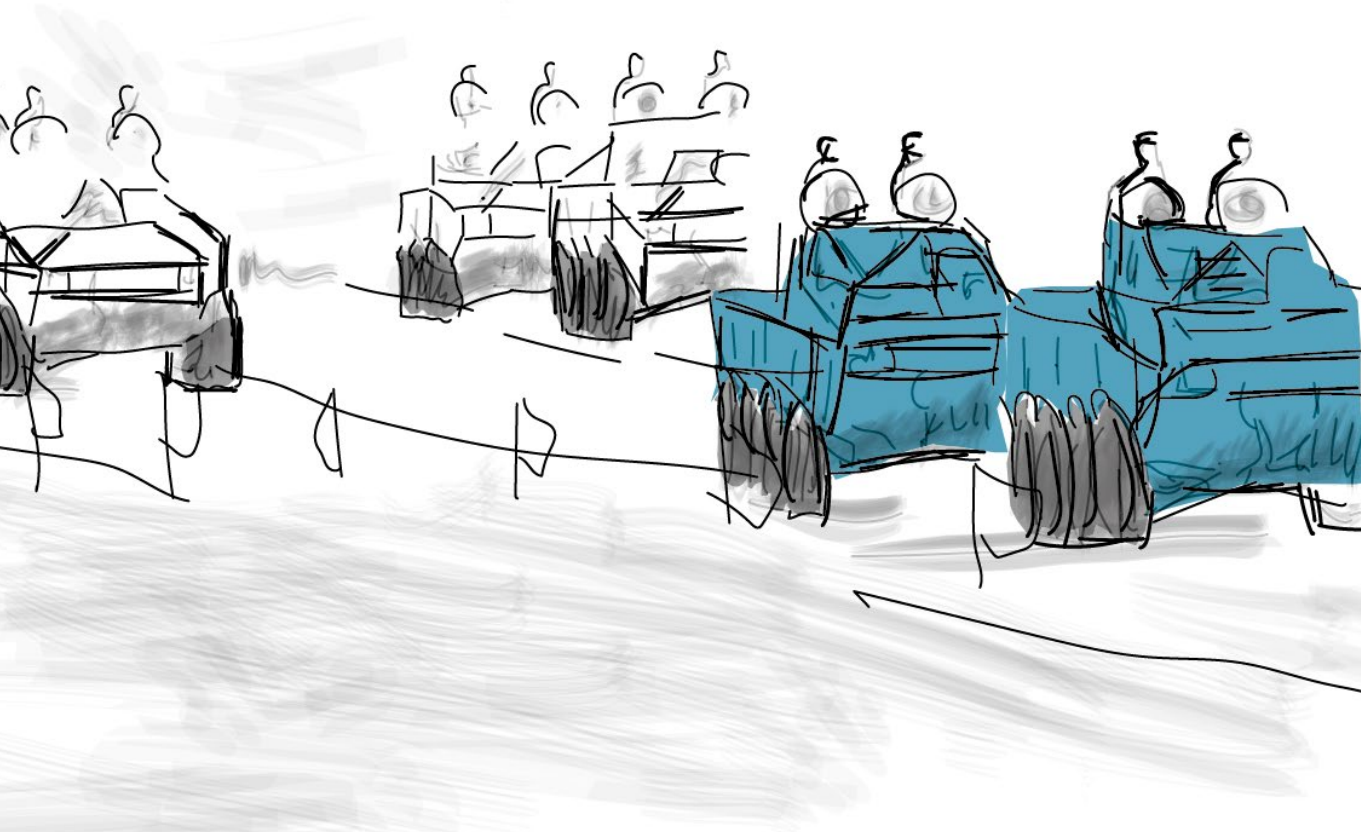
But unrest is stirring in China.

CHAPTER 10

EVERY TRICK IN THE BOOK

A story of Russia and Lithuania

by
NATASHA E. BAJEMA



Assumptions 2030

- > The United States withdraws entirely from Europe
- > Russia manages to integrate old and new technology on the battlefield
- > NATO is unprepared – both politically and militarily

Standing a few metres from his Leopard 2A9 next-generation battle tank, well hidden under the cover of thick trees, Second Lieutenant Stefan Fischer surveyed the tall, barbed wire fence stretching along the Lithuanian-Belarusian border. Through his long-range binoculars, he stared down a lone platoon of Russian T-72 Shturm unmanned battle tanks sitting idly on top of a grassy mound. They were a bit too close for his comfort.

Moving his eyes towards the evening sky, Stefan caught a glimpse of a single Russian scout drone swerving dangerously close to Lithuanian airspace before turning back around. Grunting, he lowered the binoculars, glanced back at his own tank platoon, and took several deep breaths.

All four tanks under his command sat fifty feet from the main road on the Lithuanian side of the border, well camouflaged by the forest. For the past week, his platoon had carried out a reconnaissance mission, keeping a sharp eye on the drone squadrons flying near the border. His platoon, a fearsome mix of German, Belgian and Dutch soldiers, was embedded in the 1,000-strong battlegroup operating out of Rukla, Lithuania, as part of NATO's Enhanced Forward Presence Battalion. The NATO Commander had sent his platoon to the border to serve as a warning to the Russians of what might happen if they were to try anything rash. But Stefan did not like the idea of his men serving as a tripwire for a larger confrontation.

For about an hour now, the Russian unmanned tank platoon had been perched motionless atop the small hill, only slightly elevated from his position. He knew, based on earlier video feed from his handheld scouting drone, that their command vehicle was located out of sight, just around the bend. From the moment the tanks appeared on the horizon, Stefan had not been able to shake off a bad feeling. He had immediately reported their presence back to headquarters, but Lieutenant Colonel Gerhard Mueller, his Commanding Officer, said the Russians must have just detected his platoon in the forest and moved the unit to the border as a counter-provocation.

The movements of Russia's armoured units near the Belarussian border were part of *Zapad 2030*, a week-long joint military exercise between Russia and Belarus. Moscow had made a big fanfare about its prowess in robotic and electronic warfare and its troops were exercising a number of hybrid scenarios. Defying NATO's expectations, the Russians had deployed over 100,000 troops to Belarus for the war game, a huge number that did not even include hundreds of combat-ready unmanned systems or thousands of Belarussian troops stationed along the border.

Stefan sensed this was not just a show of force by the Russians. They were practising a full-scale war against Europe with an impressive suite of advanced technologies –unmanned tanks, autonomous drone squadrons capable of swarming, and an electronic warfare company for disrupting adversary communications.

Why are they operating so close to the border? It doesn't make any sense.

"Sir, they're like sitting ducks up there," Sergeant Klaus Visser said, grinning at him from behind the machine gun at the top of the turret. He pointed two of his fingers at the tanks, pretended to take aim, and then blew fake smoke. "And didn't that drone get awfully close to crossing the border that time? It's almost like they want us to shoot at them."

Stefan nodded curtly, giving his gunner a tentative half-smile. He couldn't fully remove the grim scowl from his face or ignore the nervous feeling in the pit of his stomach. Something felt terribly off about everything.

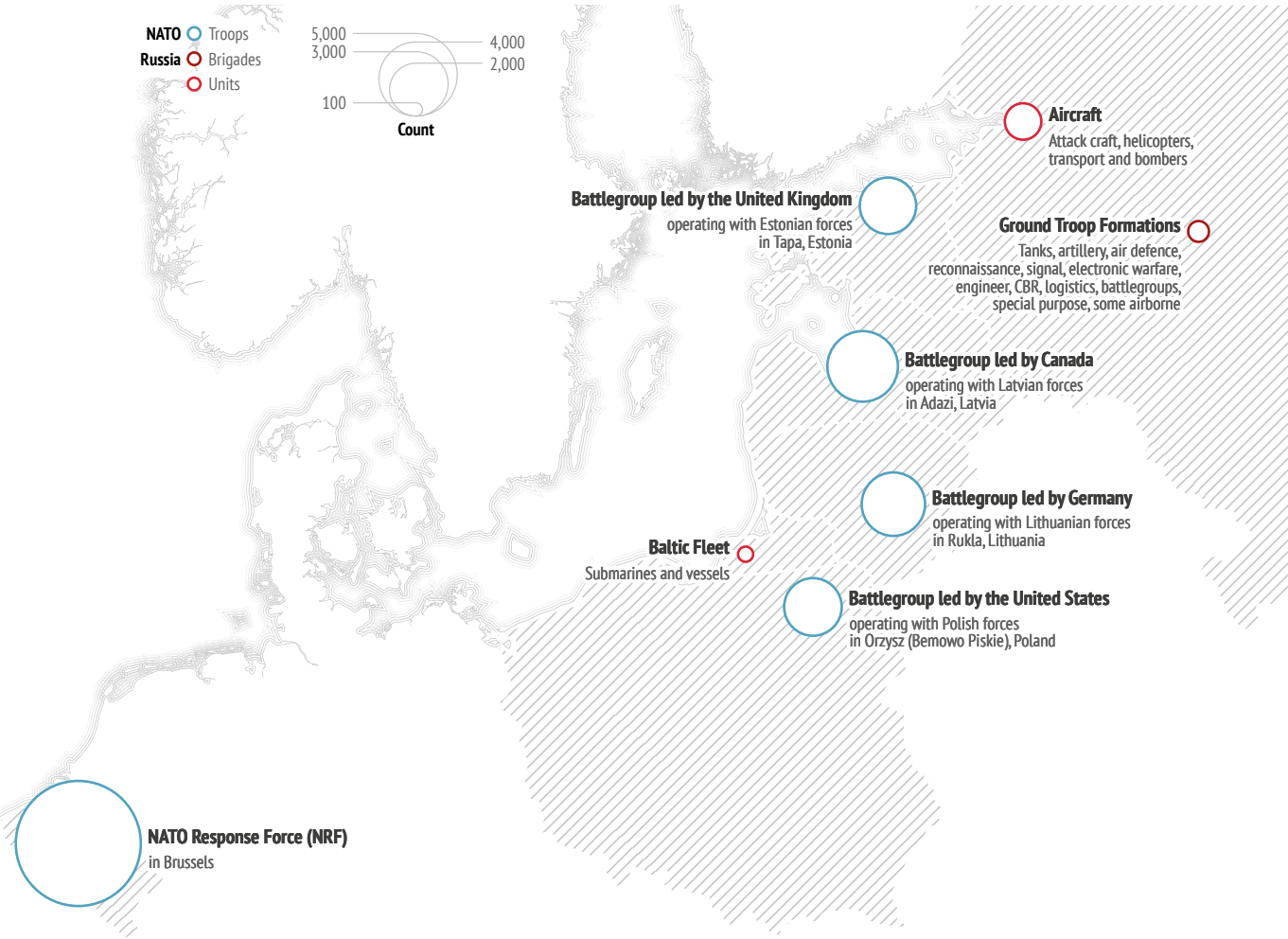
He had already voiced his concerns to his crew, and they had shrugged their shoulders. One of them yawned and said, "another exercise, another show of force by the Russians. Let me know when they really do something new and interesting." Even Klaus was sceptical and argued, "Sir, they can't afford to take the Baltics. Even if they overwhelm us in a surprise attack, the Russians can't hold the territory permanently. What good would it do them? Eventually, NATO's counterattack would push them back out of the region and that would be a devastating blow for Moscow."

Yeah... but it would take several months for the Americans to get here. That is, if they get here at all.

Ever since the US withdrew its last troops from Germany earlier in 2030, many European members of NATO had expressed their serious concerns about the strength of America's commitment to Article V. The US's military withdrawal from Europe had started already

NATO and Russia force deployment

NATO's Enhanced Forward Presence and Russia's Western Military District



NB: No detailed data on Russian troop levels available.
Data: NATO, 2020; FOI, 2019; Natural Earth, 2020

a decade earlier, but had moved forward rather slowly. Since European countries naively hoped with each presidential election that the US would eventually reverse course and bolster its presence abroad, they had failed to significantly expand their own defence spending. To their dismay, the reduction in US troops proceeded right on schedule due to a lack of broad popular support among American citizens for keeping troops overseas during peacetime.

Given the power vacuum left by the Americans, Stefan worried that Russia might finally seize the opportunity to establish a long-desired land corridor between Belarus and Kaliningrad. Although the newly elected US president was in favour of restoring America's pivotal role in NATO, she could not raise the necessary support in Congress to fund a major overseas troop deployment. Nevertheless, she insisted that America's military was prepared to come to Europe's defence if need be.

Although the president's offer was meant as reassurance, Stefan did not like imagining the available options for an American defence against a surprise attack by the Russians in a bid to grab the Baltic states. Most likely, American assistance would involve the use of tactical nuclear weapons to turn the tide of the battle, leading to a Russian retaliation with nuclear weapons on European soil.

From Stefan's perspective, there would be nothing to stop the Russians from achieving their military aims if they called the US's nuclear bluff and dared to seize the advantage. With their superior tanks and infantry, NATO forces would certainly put up a good fight, but they would be quickly overrun by a Russian force as large as 100,000.

As convinced as he was that there was something different about this exercise, Stefan was not about to report his gut feelings back to headquarters – at least not without solid evidence of Russian soldiers brazenly crossing the border and opening fire. So far, the mysterious appearance of the unmanned tank platoon was the most exciting thing that had happened all week. His team had taken many digital images of the tank from various angles and lighting, which would greatly enhance the target recognition algorithm used by NATO's autonomous drones. That meant the long trip from Rukla would not be totally in vain after all.

For some reason, Stefan could not take his eyes off the Russian tanks. He furrowed his brow again, noting their exposed position. Even for a provocation, Stefan would never have stationed his tank platoon out in the open and up on a hill. Even if they were unmanned. It was reckless and stupid.

Sighing heavily, Stefan hooked the binoculars to his jumpsuit and climbed up the side of the tank. Just then Sergeant Pierre Lamont, his driver, poked his head through the hatch. "Sir, the dashboard appears to be overheating. I cranked on the AC to cool things down, but you should probably come take a look."

Suppressing a groan, Stefan followed after Pierre, lowering himself into the hull and instinctively pulling up his nose at the familiar cocktail of odors wafting toward his face. The cramped space always reeked of sweaty gym socks, body odour, and urine, but to him, it also smelled like home.

Once situated in his bucket seat, Stefan stared up at the computer screen that usually streamed the latest ISR data coming in from NATO headquarters, providing a common operating picture for all units in the field. When his mind registered the text on the screen, his mouth fell open in dismay.

The screen was completely blank except for an ominous message in green lettering: "Repairing file system on hard drive. Do not turn off the computer."

Damn.

"The computer didn't overheat," Stefan said breathlessly, his pulse spiking. "We've been hit by a cyberattack."

"Um... Lieutenant Fischer," Klaus said over the intercom. "I think you'd better come and see this."

What now?

His heart pounding hard, Stefan stood up on his seat and poked his head through the hatch. Klaus pointed at the sky, his hand shaking. The last light of day dimmed as the sun set behind the horizon, making it difficult to see anything clearly. Stefan pulled out his binoculars, switched the setting to infrared, and gazed up at the sky. Instantly, his stomach roiled.

"They're a lot larger than the previous drones," Klaus said. "And they're heading right for the border. Do you think they mean to attack?"

"They definitely mean to do something. I'll go call it in," Stefan said. He gave Klaus a tense look. "Stay frosty up here, okay? If anything else strange happens, come back inside and seal the hatch."

Klaus nodded, swallowing hard.

Stefan lowered himself back into the hull and reached for the radio. "Command, this is RED DAWN, do you copy?"

There was static on the other end of the radio.

"Command, do you copy?"

More static.

Stefan swung his head around to look at Pierre in the driver's seat and saw that his blue eyes were as large as saucers. "I can't get through to headquarters," Stefan said grimly. "Our radio signals are being jammed."

"Everything's gone dark?" Klaus said, his face a shade paler than before.

"Well, our CVC intercom is still working," Stefan said firmly. Without wasting another moment, he called to the other tanks in his platoon, "OVERLORD, CHARLIE, BUSTER, this is RED DAWN. We've got a swarm of drones coming in hot. Comms are down. I repeat comms are down. Let's roll out."

Once Stefan received a copy from each of his tank commanders, he gave the signal to Klaus who flipped the engine switch, put the stick into gear, and released the brake. The hydraulic pump of the tank's engine groaned and whined as it whirred to life. Then they moved out from the edge of the forest and headed down the road at a good clip, following after the other tanks. Stefan exhaled sharply, relieved to be headed back to base.

Klaus lowered himself into the hull, closing the hatch above him, and Stefan looked at him expectantly.

"What's happening up there?" he asked.

"Sir, the drones have crossed into Lithuanian airspace, and they appear to be spraying liquid on the ground, just like a crop duster would. You don't think that's a bio or chem agent, do you?"

"What?" Stefan asked, his eyes growing large. He spoke quickly into his radio, "OVERLORD, CHARLIE, BUSTER, how do you copy?"

There was only static.

"They're jamming all our comms now," Stefan shouted over the din, rubbing his sweaty forehead.

An indicator light appeared on the control panel, and a loud beeping erupted. Stefan surveyed the panel and knew immediately what the alert meant.

"Goddammit!. They're releasing a nerve agent," Stefan said, his breath nearly leaving him. He could not believe the Russians would dare cross that moral boundary. It was as if they were calling NATO's bluff on their willingness to use nuclear weapons.

Pierre's eyes widened. "The Russians are attempting to gas us?" He screamed over the noise of the engine.

Stefan nodded.

"But why? We're perfectly safe from chemical weapons inside our tanks." Klaus shouted at Stefan.

Stefan contemplated the notion for a moment, and a light bulb came on. "The nerve agent must be persistent," he yelled. "They're using it as an area denial weapon."

"Area denial? But that means..." Klaus's voice trailed off.

Stefan whipped his body forward, swivelling the periscope to get a glimpse at the unmanned tanks behind them. His head jerked back with shock.

The platoon of unmanned tanks had rolled down the hill, barrelled over the border fence, flattening it to the ground, and were in hot pursuit of their platoon. Lying on the ground near the guard tower were the bodies of Lithuanian border guards.

The Russian tank at the front of the line fired a round at them, and an artillery shell ricocheted off their hull. It exploded, shaking the interior of their tank and spreading a cloud of gas around the outside.

More nerve agent.

Stefan pushed the periscope away and saw the pale look on Klaus's face.

"Permission to engage, Sir?!," Klaus shouted.

Stefan nodded. "Gunner heat tank."

"Identified," Klaus yelled.

"Fire!" Stefan shouted.

"On the way!"

Stefan peered through the periscope again and watched as the anti-tank shell pierced the hull of the unmanned tank and erupted into flames. "Target cease fire! Driver move out."

Pierre pressed down hard on the accelerator. But before the Leopard tank could reach its maximum speed, there was a loud metallic thud on the back of the hull.

Then it was as if everything happened in slow motion. The tank shook with the blast of the explosion, knocking the air out of Stefan's lungs and sucking the sound from his ears. Whirling pieces of white hot shrapnel sprayed towards him against an eerie backdrop of complete silence.

Stefan felt something sharp stab his chest and stomach, the initial searing pain followed by a calm numbness and warm liquid running down his jumpsuit. Oil and smoke filled the hull of the tank, causing Stefan to cough, wheeze, and gasp for air.

"The tank's on fire," Klaus screamed at him and pointed up at the hatch. "We need to get out of here."

Stefan shook his head slowly, his pulse weak. "We can't... the nerve agent..." he mumbled, knowing Klaus couldn't hear him.

Death before dismount.

The edges of Stefan's vision clouded, and then there was only darkness.

...

His heart heavy with grief, Lieutenant Colonel Gerhard Mueller saluted the aluminium casket draped in a German flag as it passed by him and was loaded onto the plane. His men were carrying the body of his fellow countryman, Stefan Fischer, home to the city of Hamburg where his family would bury him in his final resting place.

He knew something was wrong. I should have listened.

But Gerhard was not even sure if NATO could have changed the outcome had he done something differently. In hindsight there had been plenty of ominous warning signs, and NATO leadership had completely failed to anticipate Russia's bold move to capture a portion of Lithuania.

Its preparation disguised by the joint exercise, the Russian military operation had practically chopped the country in half and cut off three

NATO allies from land support. Before reaching Kaliningrad, Russia managed to seize the cities of Kaunas and Vilnius. Despite their massive military advantage, the Russians had largely done so using chemical warfare in blatant violation of their treaty obligations and internationally accepted laws of war.

Now that was something Gerhard had not seen coming, not in the wars of the future at least. Chemical warfare was supposed to be a thing of the past – a weapon of mass destruction eschewed by almost every nation around the world, perceived to have little value on the battlefield. But apparently, the rise of unmanned warfare now promised to give chemical agents a new life – offering an effective means to deny an adversary certain types of battle and to force them into fighting on a less advantageous front and with unmanned systems.

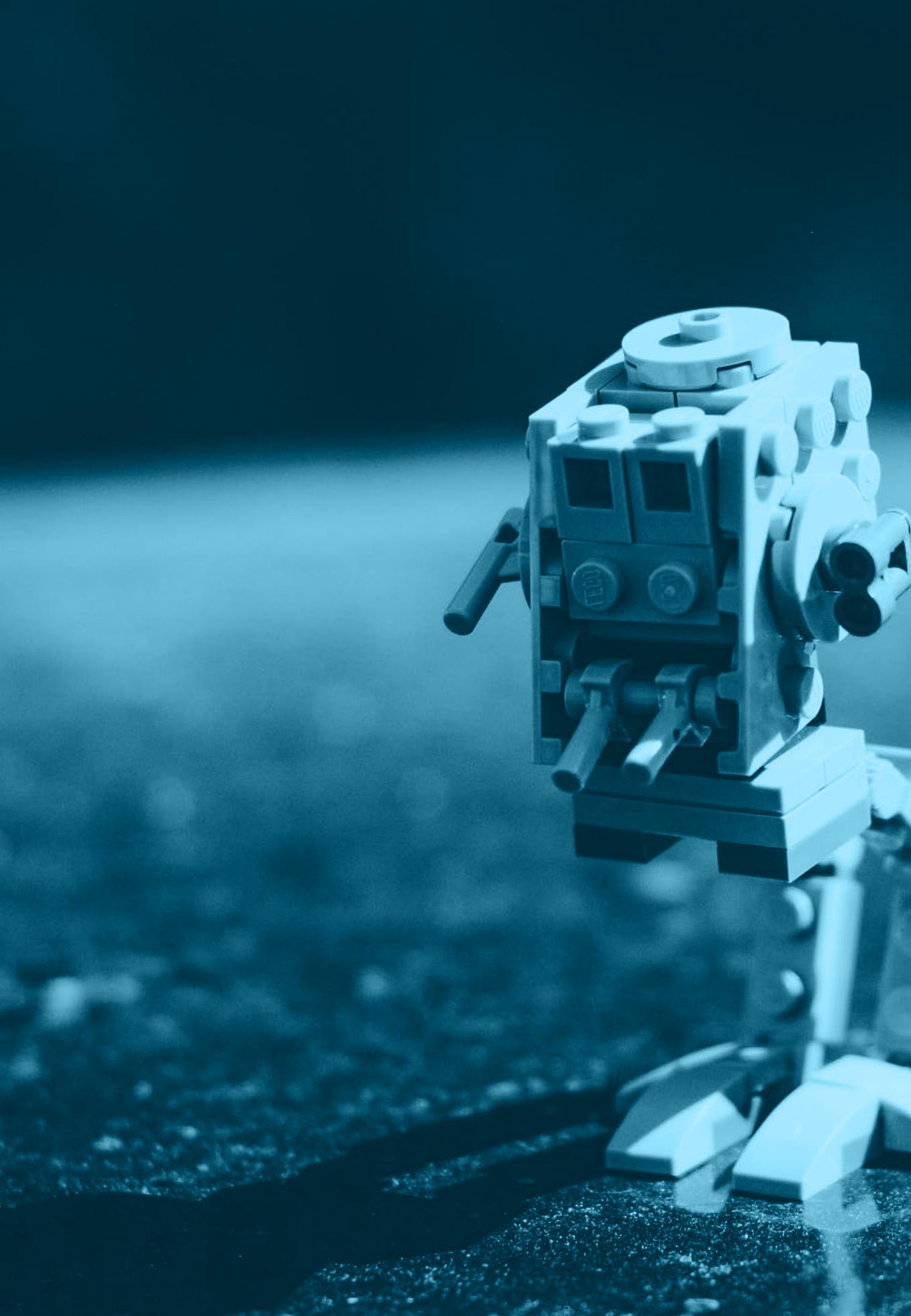
By contaminating their warpath with nerve agent and jamming NATO communications, the Russians had made it difficult for NATO forces unprepared for chemical warfare to intervene on the ground. NATO's multinational Chemical, Biological, Radiological and Nuclear (CBRN) defence battalion, stationed in the Czech Republic, required anywhere from five to twenty days of preparation to deploy and were only now en route and moving towards the Polish border, no less than two weeks after Russia's surprise attack.

Recalling how everything went down still took Gerhard's breath away. Russia's rapid manoeuvre on land had forced NATO aircraft to challenge Russia in the air, only to battle swarms of unmanned drones programmed for suicide missions. NATO losses were severe, and they were forced to concede the territory. The Russians achieved their battle aims in less than eight hours – a land bridge to Kaliningrad, a major blow to the NATO alliance, and an attempt to undermine global norms. As much as he hated the Russians for what they had done, he could not help admire them at the same time. The combination of unmanned forces, nerve agent, and radio interference reminded him of the German *Blitzkrieg* in World War II in which the deft use of radio communications had allowed German tank formations to seamlessly coordinate their attacks and overwhelm the Allied forces.

The heavy losses in NATO aircraft and casualties on the ground were not sufficient to convince the US to use nuclear weapons for fear of Russian escalation. However, US Congress did authorise sending 100,000 troops to Europe to shore up the conventional imbalance with Russia – a definite win for the alliance. But it would take the Americans about six months to get over there. Until then, NATO and the Baltic states would have to accept the new *status quo*.

Without Russia's cooperation, they would never have recovered the bodies of the NATO tank platoon lost at the Lithuanian border. The irony tasted bitter in his mouth. Mueller wondered what it would cost NATO to reverse the new situation in the Baltics and if NATO's European members were willing to pay the price.

The shrill notes of *Amazing Grace* played on a single bagpipe, bringing Gerhard back to the ceremony. The music filled the crisp air in the open hangar owned by the Lithuanian Air Force. The familiar melody of the song brought tears to his eyes as he hummed the last verse.

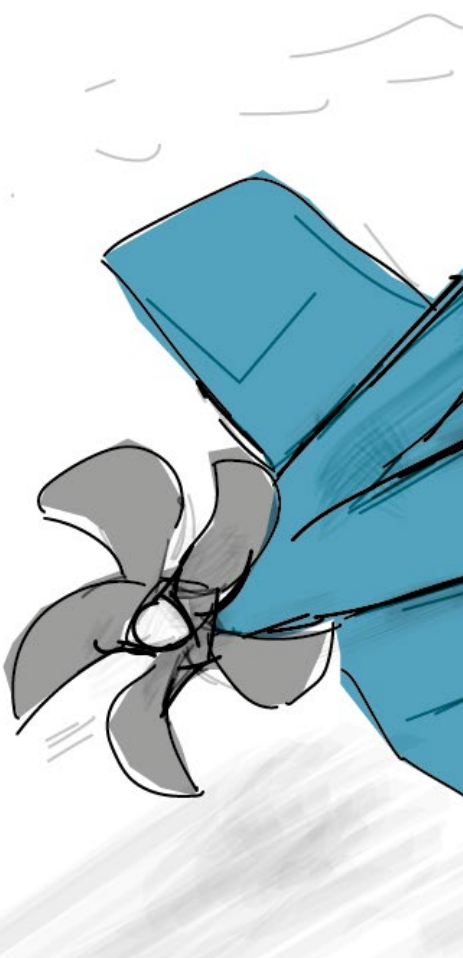


THE INGENIOUS CONFLICT: OF ISSUES AND METHODS

The ingenious conflict: of issues and methods

According to an old adage, we are doomed to fighting the last war – preparing for what we know rather than what might be yet to come. In truth, this is because conflict itself is characterised by a high degree of innovation. Not just technology might have changed since the last conflict, human use of it might be either unknown or new. Human attitudes to a host of issues, means and values might have changed, as might the landscape in which the conflict is set. It is this ingenious nature of conflict that is hard to grasp in advance.

The scenarios in this section zero in on the innovative aspect of future conflicts: where actors operate in either new environments, for reasons hitherto unknown, and with means not yet fully available. They highlight the continuously surprising aspects of conflict that, quite literally, come with the territory.

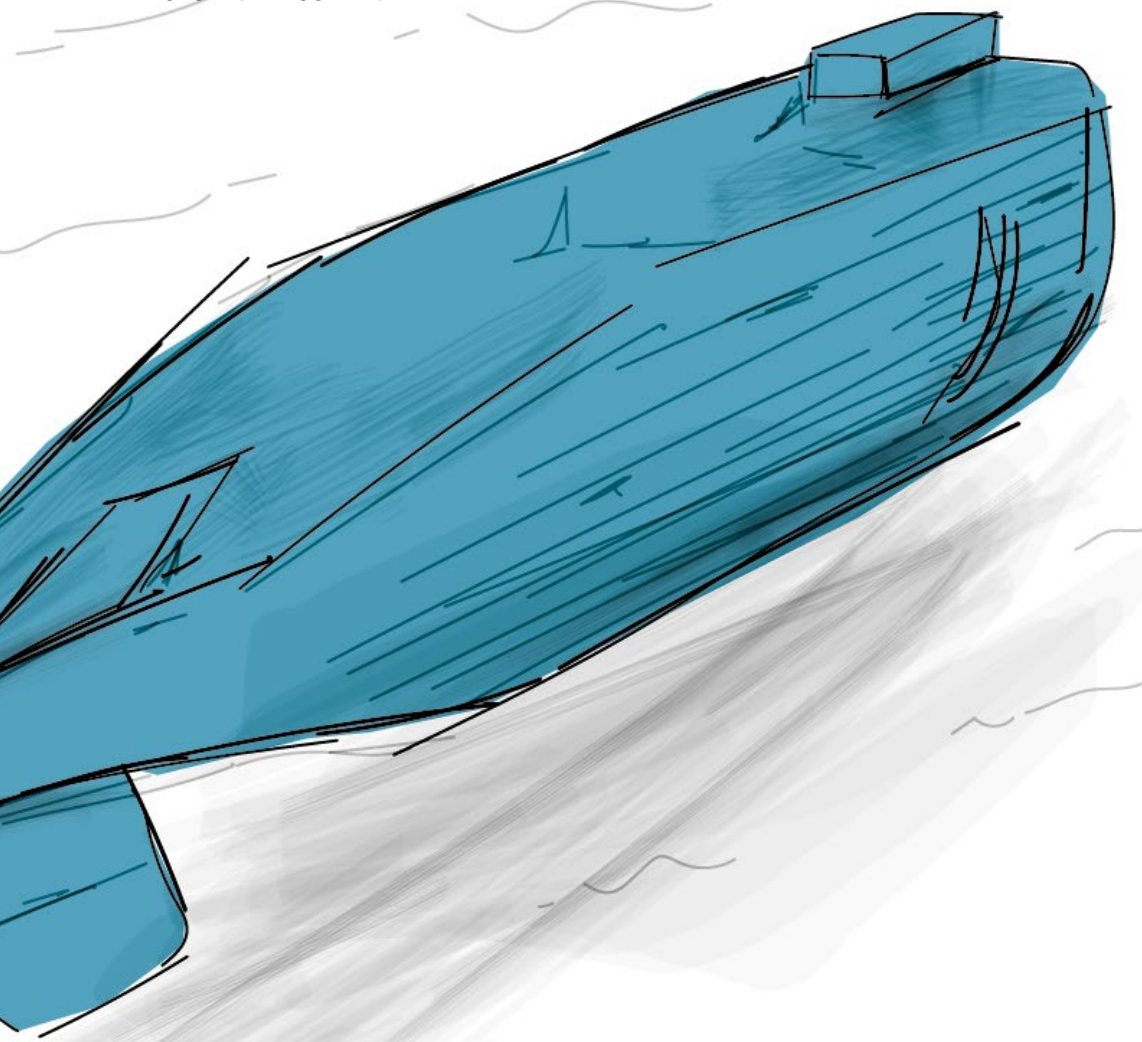


CHAPTER 11

HUNT FOR THE UNMANNED RED OCTOBER

The rise of the underwater drone

by
ZOE STANLEY-LOCKMAN



Assumptions 2030

> Hybrid conflict extends to the maritime domain

> Russian relations with Europe remain tense

> New technology creates more legal loopholes

The mysterious unmanned underwater vehicle (UUV) detected in the waters just south of Stockholm strikes Rear Admiral Bertil Larsson as unusually close to Muskö naval base. Just as he escalates the intelligence assessment from 22 May 2030 to the prime minister's office, he receives a call from Major General Åsa Nilsson. "Are you seeing this at Muskö, too?," Larsson asks, certain that the Military Intelligence and Security Service (MUST) chief is calling about the UUV by the base. No, she responds. "Our maritime picture is showing that four unidentified vehicles have been located in the Baltic Sea. All UUVs, all surfaced. Another at Muskö would make five." Sure enough, the underwater vehicle outside the naval base has surfaced, too. It is less than one metre long – smaller than the mini-submarines that have occasionally appeared uninvited in Swedish waters in recent years. To spot one would require top anti-submarine warfare capabilities and a dose of luck. To spot five, all surfaced at once, made no sense.

This is not the first time that 'little green men' have appeared in the blue, but it is the first time that Admiral Larsson's sailors have the chance to surround the intruding vehicle before it returns to open sea. The HSwMS *Karlstad* crew seizes the UUV, still unsure if it is a research vessel that has veered too close to the entrance of its base, or something more nefarious. The Cyrillic writing on the recovery float gives grounds for some sailors to speculate, but there is no flag to go by, nothing close to a grey-hull equivalent. There is speculation that connecting the trojan UUV to a computer to learn more could be exactly what an anonymous adversary wants. But there are no ways to provide answers to such speculation until the legal question is answered: what exactly is this object?

Admiral Nilsson quickly recognises the dilemma: there is no way to determine a proportionate reaction to the seized UUV without first knowing its legal status, but international maritime law is murky on the status of unmanned maritime systems.[1] He knows that classification of the object as a 'ship', a 'device' or 'equipment' has implications on how escalatory the presence of the submersible in territorial waters is, yet every state can decide on the legal status of unmanned systems for itself.[2] Regardless of the status of the UUV, what becomes clear is that it is a manifestation of a loophole in the United Nations Convention on the Law of the Sea (UNCLOS) that has been quietly ripening for exploitation. The ensuing confusion paralyses operational decision-making until the legal authority of responding to the military object can be established.

...

The most obvious event that seems linked to this incursion is the killing of eight Kremlin-affiliated paramilitaries in the Makarov Basin just ten months previously. If the UUVs are Russian, as suspected, then their presence in Swedish waters could be read as asymmetric retaliation.[3]

Geopolitical tensions in the Arctic have been rising for the past several years, especially

1 For a full description of the legal ambiguity, see: Robert Veal, Michael Tsimplis and Andrew Serdy, "The Legal Status and Operation of Unmanned Maritime Vehicles," *Ocean Development & International Law*, vol. 50, no. 1, January 2019, pp. 23-48.

2 Thus far there is only one example of this loophole on display: China seizing a US drone, which it called "unidentified equipment" but which the US argued was a "vessel." This precedent is different because (1) there was a quick diplomatic solution that meant the legal ambiguity did not escalate into a problem; and (2) the legal basis is slightly different, as the US is not party to UNCLOS.

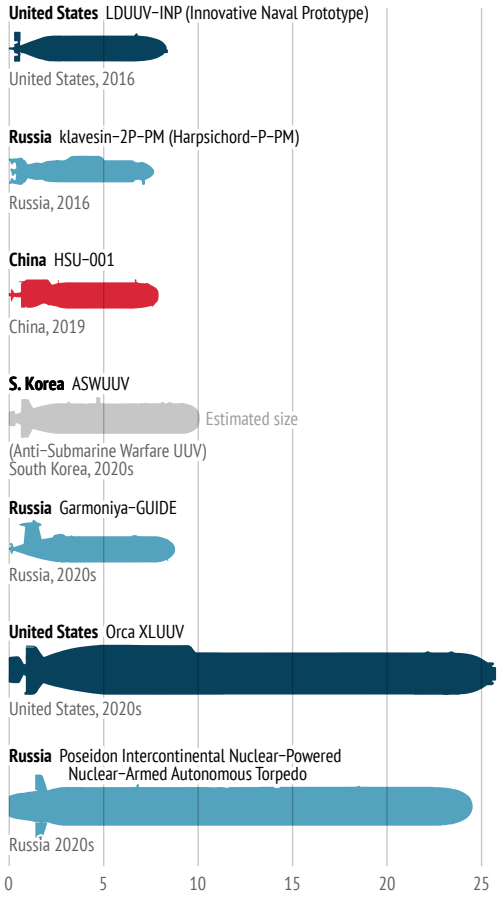
3 The Battle of Khasham serves as loose inspiration here. See: "How a 4-hour battle between Russian mercenaries and US Commandos unfolded in Syria", *New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.

since the 2027 decision by the UN Commission on the Limits of the Continental Shelf to accord territorial rights over much of the Lomonosov Ridge to Canada.[4] This UN decision should have meant Moscow could not pursue economic activities that many of its economic growth forecast models had taken for granted. Instead, it has led Moscow to resort to illegal economic activity, especially by the use of paramilitary affiliates of the Wagner Group. This came to a head last summer when the Canadian Coast Guard arrested a group of unauthorised miners, who subsequently opened fire. After eight miners were killed, Russia denied responsibility for their presence.

While not itself a claimant in territorial disputes with Russia, Sweden has found itself on the receiving end of Russian ire since it officially lost control of much of the Lomonosov Ridge. President Putin, now in his mid-70s, has reserved particular disdain for Stockholm since the Swedish icebreaker, *Oden*, proved a key asset in confirming the scientific claims that conferred the territorial win to Canada.[5] After the 2027 decision, intelligence assessments documented a shift from Russian resource-grab tactics towards post-Soviet targets, to adventurism towards other countries it perceives as robbing the Russian people of economic opportunities.

Moscow has by no means toned down its cyber and digital active measures in recent years, but connecting the unmarked UUVs with a Russian signature is also consistent with adventuristic forays in the physical domain. Russian exploitation of social media continues to be more effective against the US relative to Europe, all the more so since the European social media giant SafeSphere moved to a subscription model and introduced safeguards to slow the spread of inauthentic content. With the most popular social media company in the EU relatively inoculated against disinformation campaigns,

Large Autonomous Underwater Vehicles



Data: H I Sutton, *Covert Shores*, 2019

hybrid operations have in turn spotlighted another tool: unmarked, unmanned systems.

Robotics have become the cornerstone of Russian techno-nationalism, all the more so because Chinese science and technology (S&T) cooperation has cancelled out the impact of sanctions in select high-tech segments. Since decommissioning the *Admiral Kuznetsov* – its sole aircraft carrier – without a replacement six years previously, Russian military doctrine has emphasised smaller, more modular systems

4 Canada submitted its long-awaited claim in 2019: for analysis, see Andrea Charron, "Canada's UN submission will (eventually) draw the last lines on the map", *The Conversation*, June 5, 2019, https://theconversation.com/canadas-un-submission-will-eventually-draw-the-last-lines-on-the-map-118150.

5 Sweden has an Arctic Agreement with Canada, including collaboration to strengthen Canadian territorial claims *vis-à-vis* Russia: "Sweden and Canada sign Arctic agreement", *ANP/The Local*, December 12, 2015, https://www.thelocal.se/20151212/sweden-and-canada-sign-arctic-agreement.

similar to the ones found in the Baltic Sea. This has fed Moscow's ambitions to boost its advanced robotics capabilities, despite malfunctions reported in Russian equipment stationed in Libya and Belarus. Across the board, militaries are getting more adept at deploying autonomous systems, although Russia is one of the few states confirmed to have lethal autonomous weapons systems (LAWS). Still, regardless of the level of autonomy, no technological breakthroughs have been able to meet the insatiable energy requirements necessary for UUVs to be as advanced as other autonomous systems.

...

By early June, *Graphika* blog posts have popularised the opinion that the seized UUV matches the description of what Russia calls the *Kio*, a stealthy UUV named after the Soviet illusionist. The open-source intelligence community substantiates the assessment to a sufficient degree that it receives national attention. As all parties can agree that UNCLOS is ambiguous on the matter, Sweden is left to resort to unilateral action to enforce self-proclaimed rights. On 12 June – Russia Day – the Riksdag votes 239-127 to declare unmanned maritime vehicles as ships, regardless of whether they can transport passengers or cargo, and provides retroactive authority for Sweden to maintain the right to possession over the seized *Kio*.

With this authorisation, the Swedish Defence Research Agency, FOI, assesses the seized UUV on a hermetically sealed network. The supposed *Kio* does have a more advanced propulsion system than any European unmanned platform and hardware which clearly subverts strategic trade controls aimed at limiting Russian military capability development. Signals intelligence has long suggested that Sino-Russian S&T cooperation has concentrated on communications systems for unmanned maritime systems, a hypothesis that the presence of XiaoMi firmware on the *Kio* evinces. Over the coming weeks, analysis of the XiaoMi firmware reveals that the vehicles are designed to transmit communications to modems/sensors located up to 100 kilometres from pre-determined bearings, a feature that matches the distance for five UUVs delivering real-time intelligence on the underwater features of Muskö naval base to Kaliningrad.

But FOI is more surprised to see over-the-air software updates in the *Kio*'s code. This goes against Standardisation Agreement (STANAG) 8130, which many non-NATO countries also use for the reliability of their military equipment. Over-the-air programming is a useful industry standard for driverless cars and the like, but most militaries chose to forbid it for military systems ever since US border-patrol off-the-shelf drones were discovered to transcode data to unauthenticated devices. For NATO allies and some partner countries, STANAG 8130 explicitly forbids over-the-air updates for commercial-off-the-shelf (COTS) items – a move that has aimed to reinforce safety and security, but has meant that the speed of software updates can be subject to onerous timelines.

For the *Kio* UUVs, though, the over-the-air function lends credence to the idea that they experienced aggregate failure. This would mean that, instead of an isolated incident occurring on a single platform, a bug instantaneously replicated across all platforms that use the same code. Although the *Kio* is primarily an intelligence, surveillance and reconnaissance (ISR) platform, FOI shares its concerns over the safety of Russian military software practices with its counterparts in partner countries, specifically citing the risks of aggregate failure for Russian lethal autonomous weapons systems that private military contractors have deployed in the Arctic for the past three years.

With the new knowledge that Russia has not been hardening its COTS software, NATO commanders share the Swedish concerns that Russia has been cutting other corners on the safety of its autonomous systems in order to deploy them more quickly. Multilateral arms control negotiations and protocols for the deployment of autonomous systems have been reasonably successful at imposing hardware limitations, but software practices are seen to pose unnecessary operational risks in theatres where Russian and European forces are co-located. NATO tries to reopen the NATO-Russia Council to establish rules of engagement and protocols

for the use of autonomous systems – a proposal that goes unanswered.

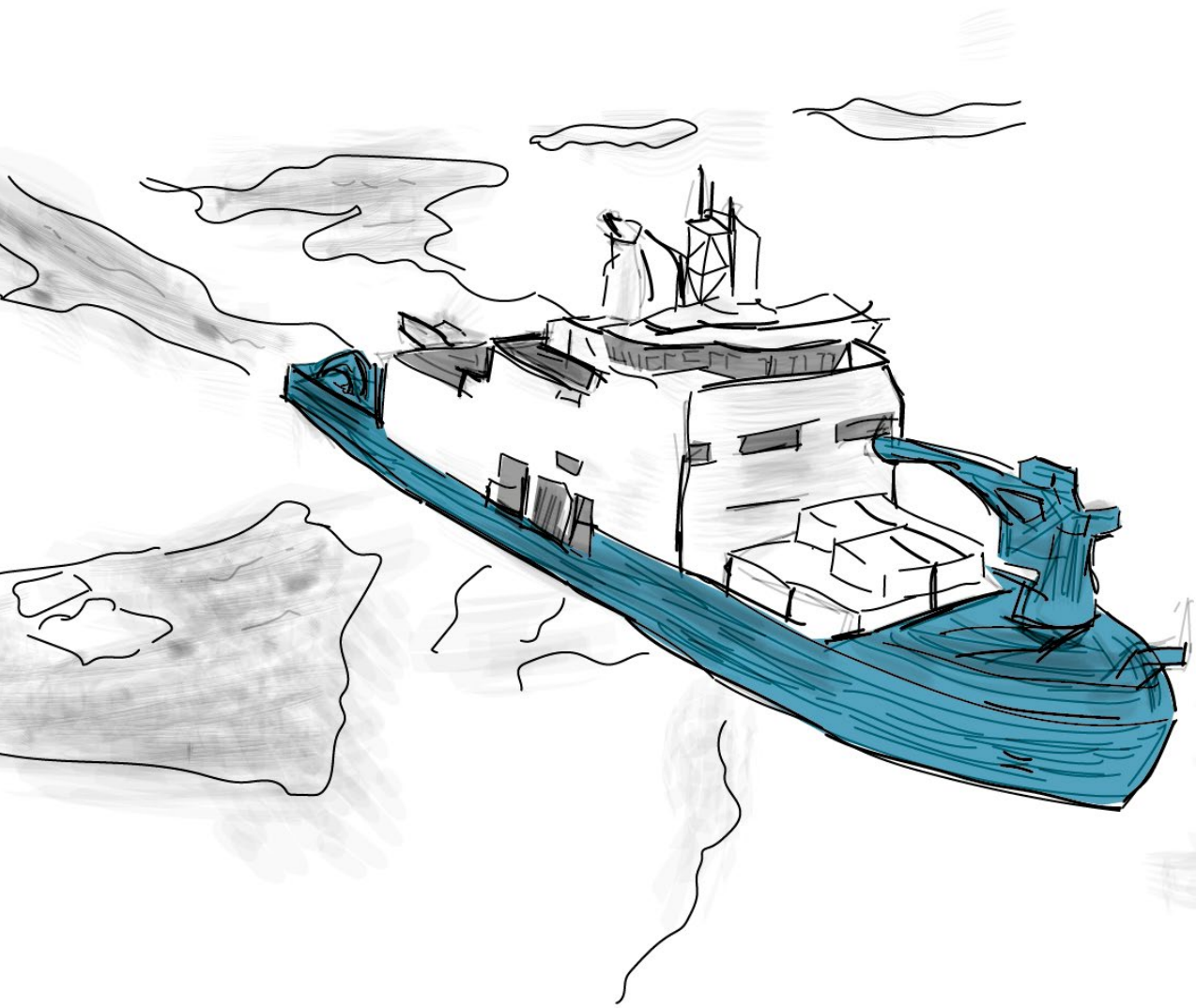
Unable to agree over the legality of the UUV deployments, operational decision-making is constrained by the inability to decide if any retaliation complies with the principles of international humanitarian law. Moreover, the time-consuming process of complying with law has occurred over the equivalent duration of several software upgrades. In the time it took Sweden to seek legal authorisation and reverse engineer the system, any valuable intelligence gathered could have been replaced. If it is indeed the *Kio*, Moscow could make the system as the Swedes now know it disappear.

CHAPTER 12

POLAR POWER PLAY

Chinese-Russian relations on ice

by
BRUNO TERTRAIS



Assumptions 2030

- > Climate change opens up the Northern Sea Route
- > New leadership in Moscow embarks on a new course
- > China's expansion is met with resistance

Even from a distance and under horrendous weather conditions, the captain of the Chinese icebreaker *Xue Long 2* could see that the *Korolev Prospekt* was in distress. The Russian supertanker, having lost its satellite positioning abilities due to a solar storm the day before, had diverged from its planned route, collided with a stray iceberg and was on fire. However, orders from Beijing were clear. Arctic Council rules and seafaring traditions be damned: China was to refrain from any rescuing operations in the region involving Russian ships. Of course, this had not been a written order, just an oral instruction given to the crew before it left port. Beijing wanted to send a clear message to Moscow that the patience of the People's Republic was running thin: Russia's insistence that it had absolute control of the Northern Sea Route and its proposal to renegotiate its oil and gas contracts with China were unacceptable.

Only two sailors died in the accident which did not create any major public outcry. In the Kremlin, however, the *Korolev Prospekt* tragedy was a moment of reckoning. The collective transition leadership was unanimous: it was time for Moscow to send a strong message of its own. As of 1 July 2030, all foreign ships were required to pay a high fee to use the Northern Sea Route – although the Russian administration would reserve the right to waive the fee for allied and friendly countries, "depending on the state of their commercial and political relations". In effect, this was a tax on the Chinese, and Beijing rightly recognised it as such. The next week, demonstrators in front of the Russian embassy brandished placards imitating the style of colonial-era "No Dogs or Chinese Allowed" signs – an urban legend given that no such sign had ever existed, but a common and efficient trope of Chinese propaganda.

...

In Moscow, a new leadership had emerged from the palace coup that ousted Vladimir Putin from power in 2027. This was certainly not a revolution in the ideological sense of the term – more a change of personnel – but the new ruling circle was smart enough to present new and more 'acceptable' faces to the world. A rotating presidency was to ensure the transition until new elections in late 2030. Former president and prime minister Dmitry Medvedev had even agreed to come back to the Kremlin as a Special Adviser, an additional reassurance to Western governments, markets and foreign investors.

The signal given to the rest of the world in 2027 was clear: Russia wanted to diversify its economy, become less dependent on its massive oil and gas exports contracts with China, and was ready to cease all support for separatists in Ukraine in order to be fully "open for business". At the same time, it was not ready to give up its claims of sovereign control of the Northern Sea Route.

By the late 2020s, more than a decade after the ice-strengthened liquefied natural gas tanker *Christophe de Margerie* made history by becoming the first commercial ship to transit the Northern Sea Route without icebreaker escort, the consequences of climate change were rapidly accelerating in the Arctic region. The North-West Passage and the Northern Sea Route became accessible to a growing number of ships during several months. This reduced transit time and distance from East Asia to Northern Europe by a third. Russia had begun to implement more stringently its Northern Sea Route Administration Navigation Rules, which included the need to request "permission" from Moscow to enter these waters.

While relations between China and Russia remained cordial and even friendly overall throughout the decade, by 2028, having succeeded in mending fences with the West, Moscow signalled to Beijing that it would like to renegotiate some of the terms of its oil and gas

Northern sea route

Data: *The Economist*, 2018

contracts with China. Moreover, Russia's assertiveness collided with Beijing's ambitions in the region. Greenland's independence in 2026 – without requesting membership of NATO or the EU – had opened the floodgates for Chinese investment on the island. Beijing's thirst for rare earths and minerals was boundless, and China had sensed an opportunity. It was welcomed with open arms by the Nuuk government.

Meanwhile, the new round of climate change negotiations between Washington and Beijing, launched by President Kamala Harris in 2025, had ended in acrimony. She was backed by an alliance of Democrats interested in putting climate change on the top of the US agenda and Republicans eager for a show of force against Beijing.

During the summer of 2029, Norwegian scientists in the Ny-Ålesund international research station on the island of Spitsbergen began noticing the arrival of a significant number of new Chinese colleagues. These were of a different style than usual: they were less talkative, did not socialise and seemed to spend their time in the large, shiny, brand new construction that

had been erected next to the old *Yellow River* building.

Since the signature of the 1920 Svalbard Treaty, the archipelago had been opened to all parties provided they did not conduct any military activity. Assisted by the intelligence services of several allies, Oslo quickly concluded that Beijing was violating the Treaty. A bland communiqué was published by the ministry of foreign affairs, reminding signatories that all parties to the Treaty were obliged to abide by its provisions and that a police investigation had been ordered. Beijing refused any inspection. Norway made it clear that it would then seek to close down the Chinese station on the island. As Beijing sternly refused, Norwegian police tried to force access into the new Chinese building in Ny-Ålesund. In the ensuing chaos, a Norwegian policewoman was killed and another severely injured. Chinese diplomacy went into overdrive: ambassadors to EU countries were sent to seek support. While Norway did not raise the matter in the North Atlantic Council, it tacitly blessed the issuance of a strong statement by the Secretary General affirming the importance of maintaining the sovereignty, integrity and security of all NATO territories, even those with a special status. In an unanticipated move, Russia stepped in to approve the Secretary General's statement and openly proposed that Euro-Atlantic nations act together to drastically limit "third parties'" military activities in the High North. Sweden warned that it could close China's Kiruna satellite ground station.

Such is the background against which the *Korolev Prospekt* tragedy unfolded nine months later.

On July 25, the Russian GLONASS satellite positioning system went dark. Russian operators were confused and could not understand what had happened. However, this was clearly a focused attack since no other satellite was inoperative.

The next day, the Russian president, acting on another unanimous Kremlin decision, called the White House on a secure line. He had a plan in mind, but one which would require the full cooperation of Washington. His US counterpart gave his blessing. Freedom of navigation was a sacred principle for a maritime power and even though the US Senate had never ratified the UN Convention on the Law of the Seas, Washington had vowed to abide by its principles. Nevertheless, this was a golden opportunity to make China pay after the gruesome murder, the week before, of a US diplomatic attaché in Beijing – who was the number three in the local CIA station. The contours of a cooperative agreement were drawn: both navies would monitor the Bering Straits for Chinese ships – which were now likely to be under flags of convenience – coordinate through the US-Russia naval incidents at sea hotline, and interdict their passage, by force if necessary.

On 15 August, the Russian frigate *Admiral Chichagov,* operating in the Eastern Mediterranean, was hit by two torpedoes and rendered inoperative. US and European intelligence confirmed that a new-generation stealthy Chinese navy submarine had passed through the Straits of Gibraltar a week before.

On 30 August, Russia closed its border with China and suspended all deliveries of oil and gas to its neighbour.

...

A few days later, while refraining from admitting guilt, Beijing quietly conveyed the message to Moscow that it would order an "inquiry" into the "tragic incident" which had led to the firing of live torpedoes "without the consent of the central military staff".

An extraordinary EU-NATO meeting took place in Brussels "to take stock of the evolving situation in the High North", leading to the creation of an 'EU-NATO evaluation and coordination centre'. Simultaneously, the EU, Norway and Russia resolved to settle their longstanding disputes regarding fisheries management and fishing rights in the Svalbard region.

In 2031, Washington quietly approached Nuuk to discuss "issues of mutual interest regarding the economic development of the country, its security and that of the surrounding areas". The discussions began in Reykjavik in June.

Things did not go well. One day, a tired US negotiator remarked jokingly that "we could still buy the island, you know!" In February 2032, the Greenlandic authorities decided to terminate any US economic and military presence on the island. One month later, Nuuk signed a thirty-year strategic partnership with Beijing, leasing parts of its territory to China for "mining and various research activities". The agreement also included the construction of a massive naval base.

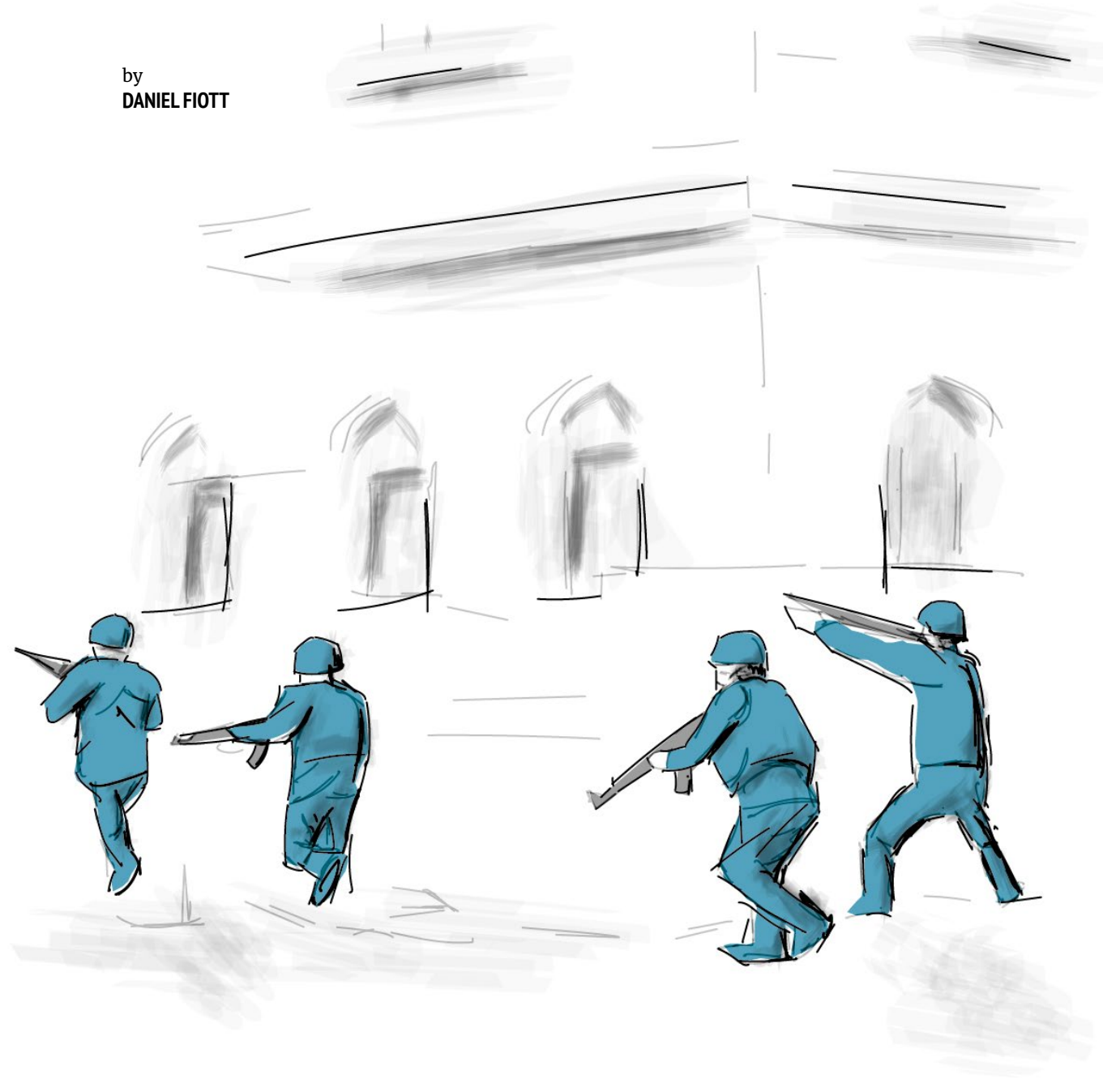
By 2032, the NATO-Russia Council had, in effect, superseded the North Atlantic Council as the main decision-making body for security in the Euro-Atlantic region.

CHAPTER 13

VIRTUAL CONGO

Or the limits of technological superiority

by
DANIEL FIOTT



Assumptions 2030

- Modern technology is useful for military training and situational awareness
- Urban, low-tech conflict cannot be won with modern technology alone
- Non-state actors use cheap yet effective technology in conflict
- Third powers may influence conflicts by flattening any technology asymmetry that exists
- Europe has the military capability and will to deploy

"Damn it!" Hidden behind an armoured vehicle, and looking down at the private's blood-soaked body, Corporal Kohler began to breathe heavily as bullets whistled past his head. It was the sixth man he had lost this week. As he looked at the court house located in the Poto Poto neighbourhood, he could hear the hum of a distant helicopter, which was soon to land in an adjacent field to the Congolese national civil aviation authority. As the smoke from the flare bellowed into the air, his comrades shouted: "prepare to board the aircraft before we are overrun!" As he ran towards the helicopter he was shot in the head by a sniper. Taking off his headset, Kohler let out a sigh of relief and regained his composure. "OK, this is really getting realistic now... I mean, I am supposed to be dead, right?"

Kohler had already seen active duty in Brazzaville and he had been advising Paris and Berlin on its military Virtual Reality (VR) programme – called 'Project Adelphi' – since the late 2020s. Project Adelphi was initially set up to enhance cyber defences, but by the late 2020s the project had moved on to a second phase of development that assisted operation commanders with the use of VR technology. The VR system would receive live situation feeds from troops based in Brazzaville, and the information was converted into realistic pre-deployment training scenarios for troops. In a sense, the Europeans were fighting a real and virtual war at the same time.

"It's getting better", he said, "but it gets dark much earlier in Brazzaville and there is something not quite right about the red hue used for the evacuation flares."

The reality was that the Europeans needed all of the technological help they could get. Europe's forces had been fighting the militias of the Congolese Party of Labour (CPL) and their allies on the streets of Brazzaville since 2028, but without making any headway – they were winning the virtual war, but losing the real one. War erupted in Congo in 2027 following the death of President Denis Sassou Nguesso in late 2026. Although Nguesso had likely died from natural causes, CPL supporters cried foul play and propagandists hit the government-run *Radiodiffusion Télévision Congo* to blast opposition forces for poisoning him. They even blamed 'foreign imperialist powers' for conspiring to overturn socialism.

The mind-boggling dimension to the war, however, was that despite the Europeans' technological superiority they were still hemmed in in Brazzaville and had not ventured outside of the security parameter set up around the Eurocorps headquarters at Maya Maya airport. Pointe-Noire and the rest of the country was still in CPL hands. While it is true that the CPL utilised guerrilla tactics, it was as if the militias were always one step ahead of European forces on intelligence. So, for example, when intelligence assessments showed that CPL militias were planning to attack the World Health Organisation office on Avenue du Général De Gaulle, the attack would take place at the Palais des Congrès on Boulevard des Armées instead. For all of the advances embodied by Project Adelphi, European soldiers were still coming home in body bags at an alarming rate and this had badly affected morale. Many European troops half-joked that a trip to Brazzaville was a 'one way ticket'.

...

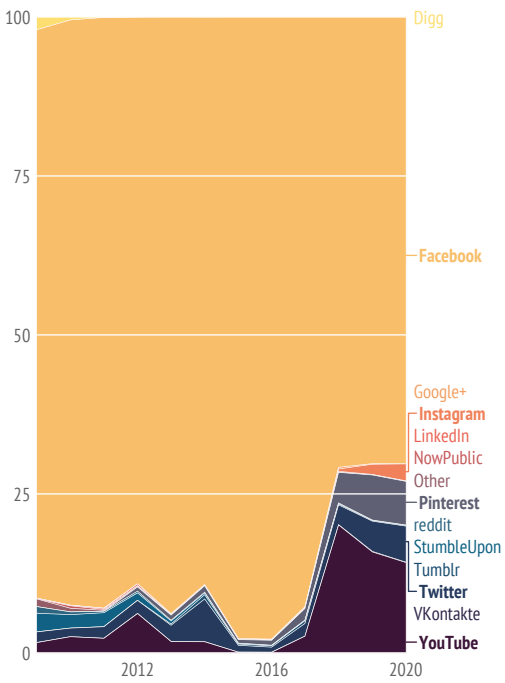
The summer of 2030 was the bloodiest phase of the conflict for the Europeans – since their deployment in 2028 Eurocorps had lost 400 troops. It was a brave political decision by European leaders to deploy Operation Vanguard in

the first place, and although critics had accused European governments of only wanting to protect their oil interests in Congo, the operation began as a genuine peace-keeping deployment to separate the CPL and opposition Pan-African Union for Social Democracy (UPADS) militias. The death of President Nguesso was the trigger for the conflict, but the reality was that his death exposed deeper problems such as years of poverty and inequality and the huge loss of oil revenues given chronically low crude prices throughout the 2020s – Congo relied on oil for 50% of its GDP.

Early in 2030, the fighting intensified as the UPADS called for the exiled Mireille Lissouba – who had replaced her late father as the head of the party – to return as the rightful leader of Congo. The CPL was also rejuvenated as it acquired ever more sophisticated weaponry that docked in Pointe-Noire. Additionally, the Chinese government announced a new round of debt relief for the country, which alleviated the financial strains. Many had thought that the Chinese would intervene militarily themselves, and they had every reason to given their close relationship with the CPL. The 2026 Beijing Summit of the Forum on China-Africa Cooperation (FOCAC) had stressed the importance of Congo to the Belt and Road Initiative, and it was no secret that Beijing wanted to invest in port infrastructure in Pointe-Noire - there were even reports that China wanted to build its first Atlantic Ocean naval base there. Yet, the Chinese resisted the temptation to directly intervene.

Approximately 1,200 Eurocorps troops were deployed to Brazzaville, and in 2030 they were still locked down in the capital. CPL forces had cut off the two major roads (the RN1 and RN2) into the capital and Maya Maya airport was the only safe logistical spot for the Europeans. Eurocorps patrols would leave the safe zone near the airport for regular reconnaissance trips, but it was still too risky to venture too far. The population density of Brazzaville did not help. The 1.7 million residents living in the city accounted for more than a quarter of Congo's total population, and sanitary conditions and the built environment of densely packed houses made the combat zone rather inhospitable.

Social media use in Africa
2009–2020, %



Data: Statcounter, 2020

However, 2 years after the initial deployment European forces were still on the back foot and Project Adelphi was not helping with military intelligence gathering. For example, in the spring of 2030 it was made known to Eurocorps that CPL forces had taken up command posts in Brazzaville's 9 major hospitals. Yet when European forces decided to storm the *Hôpital d'Instruction des armées de Brazzaville*, CPL snipers picked off troops from high rise buildings on Avenue de l'Amitié. Eurocorps forces believed that recently installed CCTV cameras were feeding information to CPL forces, but most were taken out and still CPL forces were one step ahead. What is more, when Eurocorps attempted to run public communication campaigns through text and internet messages frequent communication blackouts would occur at the same time. Such blackouts would never occur when the CPL were running their own public strategic communication campaigns.

...

By mid-2031 the game was up for European forces. After three years of combat in Brazzaville, and following the loss of over 520 soldiers (among them Corporal Kohler), Eurocorps governments were calling time on Operation Vanguard. This decision was not taken lightly, but a major media report by *Le Monde* and the *Süddeutsche Zeitung* gave no option. The special report stated that European forces were being outwitted in Brazzaville by a smartphone app called 'Clé'. This was hardly news, as recovered smartphones had revealed that Clé was used as the primary communication tool between CPL forces. European intelligence also knew that CPL fighters used Elikia and Moke smartphones, which were produced by the Congolese tech-firm VMK – the company shipped generic phones in from Shenzhen, China, before stamping them with 'Made in Congo'.

This was not the real story, though, as it was revealed that Clé was not just a messaging app – it was actually used as a geolocation tracker of all European troops based in Brazzaville. No wonder CPL forces could target European troops so easily and deceive them so readily in Brazzaville's labyrinthine streets. All of the communications and sensor technologies used by Eurocorps forces – from smart watches to satellite communications – were being used by CPL militias to pick off European troops. Clearly, VMK did not possess the technological know-how to make this work and the *Le Monde* and *Süddeutsche Zeitung* report revealed two further pieces of earth shattering news.

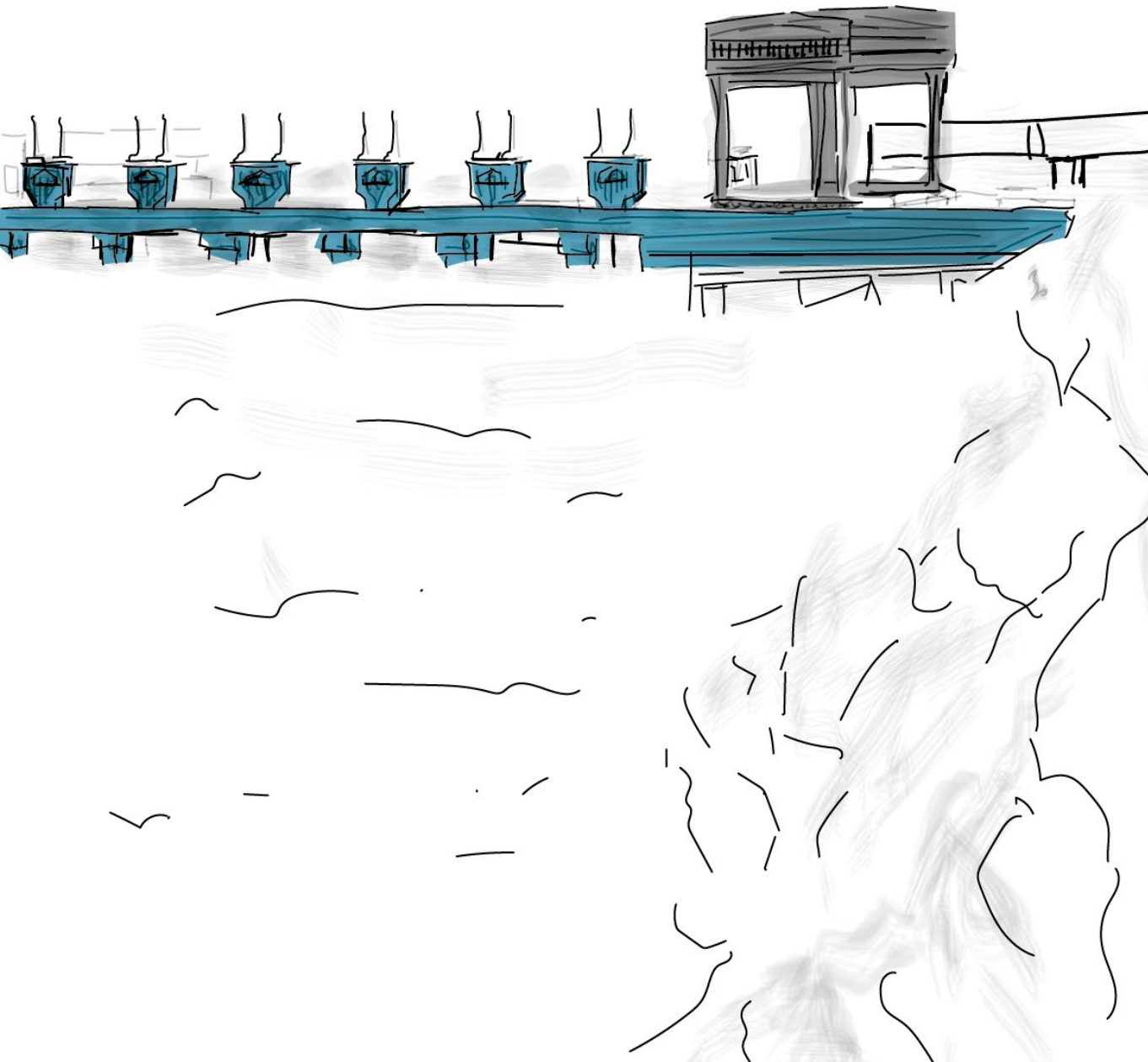
First, according to reliable sources Clé was connected to a mainframe system colloquially called 'Écluse'. It was not clear how Écluse functioned but the theory was that it was a supercomputer system that combined geolocation tracking data with other information stolen from European forces. The report went on, secondly, to reveal that Project Adelphi's VR scenarios had also been hacked by a foreign intelligence service. As Adelphi was using real-time battle information to help European forces gain more situational awareness of the conflict in Brazzaville, it was simultaneously being hacked to reveal European tactics and strategic assessments. The more and more Europeans learned about the war through Adelphi, the more and more Écluse would relay the information to CPL handsets via the Clé app. Beijing had denied any role, but it did not matter: Europe had lost both its virtual and real wars.

CHAPTER 14

SYRIA

The Chinese reload

by
LOTJE BOSWINKEL



Assumptions 2030

- Environmental concerns trigger violent conflict
- Russia still present in Syria
- China increases its economic presence
- Syrian reconstruction is very uneven

It was around 03.00 am on 20 July 2030 when phones started ringing inside the Dubai office of Frontier Services Group, a Chinese private security firm.[1] In Beijing, Executive Director Mr Ko Chun Shun had just woken up and was reading *Xinhua* news. This morning's headline: President Xi Jinping's visit to Tripoli, for the official opening of the Lebanon-Syria railway. Mr Ko, too, was soon to receive a call. He was informed that three days earlier, on an exceptionally hot morning, fishermen had detected an ash spill from the recently opened China-funded Al Aqra 660 MW coal power plant into Lake Assad.[2] That same night, hundreds of protesters gathered in front of the plant as well as at one of the compounds for Chinese workers located just outside of Aleppo city. When the authorities announced the following day that 30% of Aleppo's drinking water had been polluted – and shortages were already high as northern Syria faced a two-month drought – the situation quickly deteriorated. On the second night, tens of thousands of protestors took to the streets of Aleppo, chanting "Syria belongs to the Syrians!" and "out with the Chinese!" On 22 July, things turned violent, as Chinese workers on their way to the coal plant were dragged out of a van. All five workers and the driver were killed by the mob. Elsewhere in the city, panicking Chinese security workers started shooting on the masses that had gathered in front of a Chinese telecommunications office and an electricity construction site. Three bombs reportedly exploded – the whereabouts of the explosions and the perpetrators unknown.

Damascus reassured Beijing and deployed 10,000 troops to the city. These could not prevent the deaths of 42 Chinese workers and extensive damage to various infrastructure facilities over the span of one week. Under pressure from a massive domestic public outcry over the deaths of the Chinese workers, and advised by Moscow, Beijing sent in three Su-35 and two J-20 fighters on 27 July. But the initial three-day aerial bombing campaign, meant to swiftly quell the rebellion, did not achieve its goal. Instead, it further stirred public anger, which rapidly spread through the city and the countryside around Aleppo. Soon things went from bad to worse: inexperienced in dealing with conflicts of this sort, and in close liaison with President Putin, Xi quickly stepped up involvement, sending three additional stealth fighters, increasing bomb loads, and expanding the list of target sites. After years of successfully intensifying economic ties while carefully avoiding being dragged into the region's conflicts, Beijing's tactics had run out of luck.

…

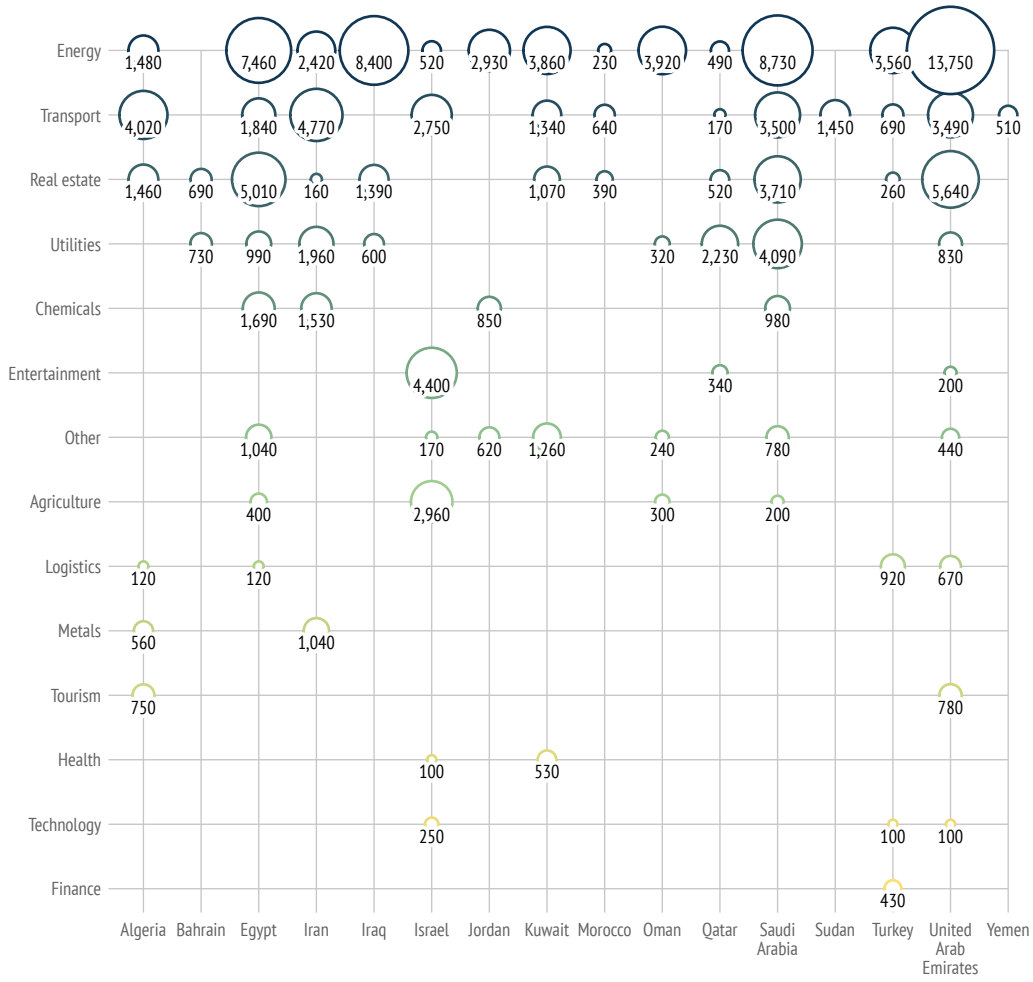
During the early 2020s, continued unrest coupled with mounting economic hardship had undermined Iran's international clout. As a result, a host of militias operating inside Syria and Hizbullah's military branch saw their funds quickly dry up, and power in Syria became increasingly centralised, a turn of events welcomed by Putin and President Assad. Israel, in turn, halted its Syrian operations in early 2022. Thanks to these developments, Damascus, even though it had relied heavily on Tehran's support throughout the war, fared surprisingly well: a relative calm returned to the country, mitigating some of the economic effects

1 Sergey Sukhankin, "Chinese private security contractors: new trends and future prospects", The Jamestown Foundation, *China Brief*, vol. 20, no. 9, May 15, 2020, https://jamestown.org/program/chinese-private-security-contractors-new-trends-and-future-prospects/

2 Meir Alkon et al., "Water security implications of coal-fired power plants financed through China's Belt and Road Initiative", *Energy Policy* vol. 132, September 2019, pp. 1101-1109.

China's Belt and Road Initiative in the Middle East and North Africa

BRI investments and construction contracts, October 2013 – June 2020



Data: China Global Investment Tracker, American Entreprise Institute, 2020

of Covid-19[3] and various sanctions regimes.[4] Syria's recovery – albeit fragile and slow – was finally underway.

Beijing began to gradually scale up engagement through its Belt and Road Initiative (BRI). In November 2024, the state-owned COSCO Shipping Lines acquired a 21% stake in Latakia port, and in March 2025 a similar stake in the port of Tartus. Encouraged by these successes, China began an ambitious infrastructure plan for a road connecting the two Syrian ports with the seaport of Tripoli, firmly in the hands of the China Harbour Engineering Company (CHEC), and a railway linking Beirut and Tripoli to Homs and Aleppo. The latter was to eventually stretch further westward, extending Beijing's

3 International Monetary Fund (IMF), "COVID-19 poses formidable threat for fragile states in the Middle East and North Africa", May 13, 2020, https://www.imf.org/en/News/Articles/2020/05/13/na051320-covid-19-poses-formidable-threat-for-fragile-states-in-the-middle-east-and-north-africa.

4 Martin Chulov, "US 'Caesar Act' sanctions could devastate Syria's flatlining economy", *The Guardian*, June 12, 2020, https://www.theguardian.com/world/2020/jun/12/us-caesar-act-sanctions-and-could-devastate-syrias-flatlining-economy.

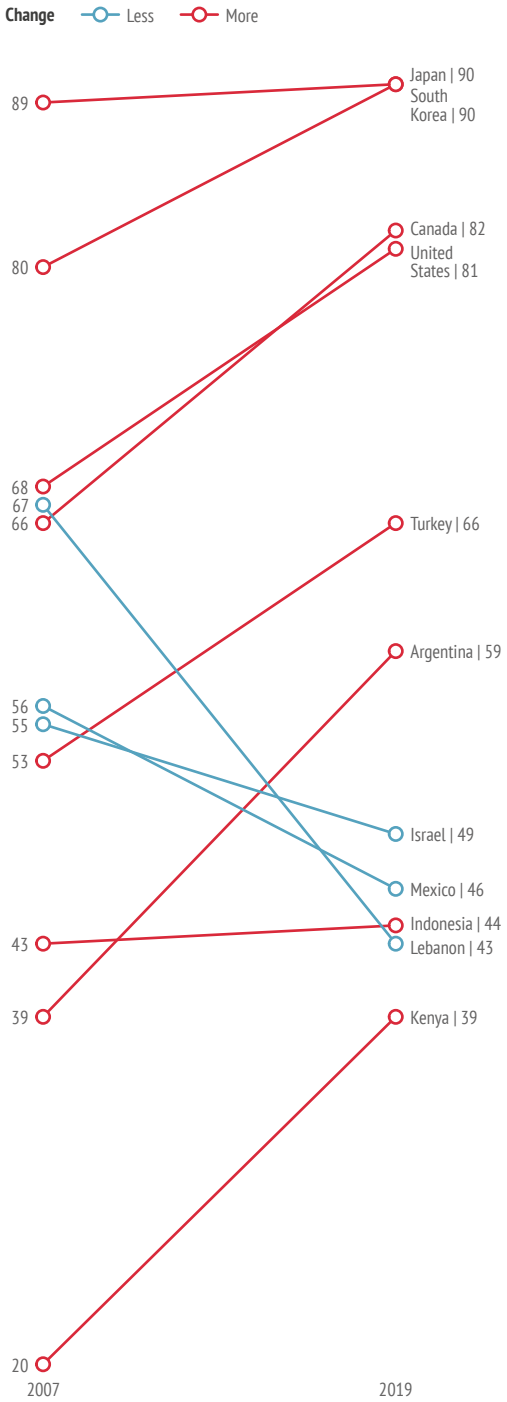
land corridor all the way from Beijing through Central and West Asia to Europe.[5]

Moscow, officially still Damascus's closest friend, was not overly enthusiastic about the Chinese expanding their economic foothold in the country. In particular, Beijing's stake in the port of Tartus was eyed with a mixture of wariness and annoyance.[6] Yet unwillingness to step on Beijing's toes and a lack of resources left Russia empty-handed. Growing Chinese influence – albeit economic – was a cause for concern in Washington, which continued to show firm commitment to the Caesar Act. It blocked various joint proposals by Moscow and Beijing in the Security Council for measures aimed at bolstering Syria's economic recovery, including the easing of sanctions. A situation where these powers would reap the benefits of a recovering Syria and increase their influence in the region was to be avoided at all cost, the reasoning went. Amidst these developments, the EU found itself in a difficult position: it wanted to allow for some level of economic development and recovery without legitimising the Syrian regime.[7] The result of this balancing act was mainly inaction.

While Chinese investments brought a new sense of optimism to Syria, they were not without controversy. In the absence of an international approach to the country's reconstruction, the Chinese projects added to the country's fractured rebuilding[8] and fed into the highly corrupt system as they stimulated graft and

Increasing worries about China's growing military in many nations

People who say China's growing military is a bad thing for their country, %



Data: Pew Research Center, 2019

5 "Is it China's turn to wield influence over Lebanon?", *Belt and Road News*, June 3, 2020, https://www.beltandroad.news/2020/06/03/is-it-chinas-turn-to-wield-influence-over-lebanon/

6 James M Dorsey, "Syria lures, but will Beijing bite?", *Asia Times*, June 14, 2020, https://asiatimes.com/2020/06/syria-lures-but-will-beijing-bite/

7 International Crisis Group, "Ways out of Europe's Syria reconstruction conundrum", November 25, 2019, https://www.crisisgroup.org/middle-east-north-africa/eastern-mediterranean/syria/209-ways-out-europes-syria-reconstruction-conundrum.

8 Joseph Daher, "The paradox of Syria's reconstruction", Carnegie Middle East Center, September 4, 2019, https://carnegie-mec.org/2019/09/04/paradox-of-syria-s-reconstruction-pub-79773.

rent-seeking behaviour among Syria's elites.[9] Moreover, Beijing's shrinking BRI budget[10] meant low social and environmental standards, fuelling anger among Syrians. Furthermore they found that their markets were flooded with overpriced goods of inferior quality.[11] In Aleppo, the once rebel-held east – which had suffered most of the war's destruction[12] – was almost completely neglected in reconstruction efforts.

This situation was not helped by the fact that Syria's population quickly expanded, not least thanks to Erdogan's decision to push refugees out of Turkey in March 2021. In Aleppo, the population increased from 1,754,000 to 2,993,000 between 2018 and 2030, with an extremely high annual growth rate of 4.5%. To illustrate: only six of the world's 548 cities with at least one million inhabitants in 2018 experienced higher growth rates in the years leading up to 2030.[13] As the countryside's inhospitable conditions proved unsuitable for resettlement, returnees turned to Aleppo's poorer (and war-damaged) neighbourhoods – in fact, the eastern part of the city. Resentment spread rapidly.

Turkey's involvement in the war stretched further. The percentage of Turks worrying about China's growing military might had been steadily rising, from 53% in 2007, to 66% in 2019,[14] and to 75% in 2028. Turkish ambivalence towards Chinese economic influence was high, too, especially compared to other countries in the Middle East: in 2019, 44% of Turks disapproved of Chinese investments, compared to 22% in Tunisia, 27% in Lebanon, and 26% in Israel. By 2028 this percentage was up to 54%, compared to increases of only a few percentage points elsewhere in the region. Turkey's wariness towards Beijing stemmed mainly from its own regional aspirations, the continued maltreatment of the Uyghurs and, increasingly, China's energy and counterterrorism cooperation with Kurdish factions in both Iraq and Syria. It was thus perhaps unsurprising that in the summer of 2030 – once again – money, weapons and fighters flooded into Syria from its northern border.

Then there was another, perhaps more unexpected, source of money that financed local war efforts: the global network of radical environmentalists called Green Resistance, with funding coming mainly from Europe but also Peru and Australia. One of its radical branches, named Earth's Last Crusaders (ELC), had been linked to a series of assassinations in the late 2020s targeting bankers, CEOs and other prominent figures involved in major gas and oil investments. ELC was also suspected to be involved in recent cyberattacks targeting various Chinese BRI power plants and industrial zones in Southeast Asia and Africa.

...

Beijing undoubtedly made the typical newcomer's miscalculation of military overreaction, yet it was determined not to make the classic superpower mistake of being dragged into an interminable war in West Asia. It decided to quickly cut its losses and make its way out. By 2031, all Chinese workers and private security personnel were evacuated, and infrastructure projects abandoned or sold at knockdown prices to Russian or Syrian companies. Elsewhere in the region, too, Beijing revised its BRI policy, halting new investments and downscaling

9 Helena Legarda and Meia Nouwens, "Guardians of the Belt and Road: The internationalization of China's private security companies", *Merics China Monitor*, August 16, 2018, https://merics.org/en/report/guardians-belt-and-road.

10 Salvatore Babones, "China's superpower dreams are running out of money", *Foreign Policy*, July 6, 2020, https://foreignpolicy.com/2020/07/06/china-superpower-defense-technology-spending/

11 Robin Mills, "Iran's deeper partnership with China is not all that it appears to be", *The National*, July 12, 2020, https://www.thenational.ae/business/comment/iran-s-deeper-partnership-with-china-is-not-all-that-it-appears-to-be-1.1047946.

12 REACH, "Syrian Cities Damage Atlas", March 16, 2019, https://reliefweb.int/sites/reliefweb.int/files/resources/reach_thematic_assessment_syrian_cities_damage_atlas_march_2019_reduced_file_size_1.pdf.

13 United Nations, Department of Economic and Social Affairs, Population Division, "The World's Cities in 2018 – Data Booklet", 2018, https://www.un.org/en/events/citiesday/assets/pdf/the_worlds_cities_in_2018_data_booklet.pdf.

14 Pew Research Center, "China's economic growth mostly welcomed in emerging markets, but neighbors wary of its influence", December 5, 2019, https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcomed-in-emerging-markets-but-neighbors-wary-of-its-influence/

ongoing projects. It resorted to its more cautious approach of the late 2010s, focusing on more stable and strategic regions.

Meanwhile, something long-overdue happened: feeling encouraged by the withdrawal of China, protestors turned – once again – against the Syrian government. This time Moscow, warned by Beijing, did not step in to back the regime. And so a few months into 2031, Assad's government fell, at last – exactly 20 years after the Syrian civil uprising had begun. Under the auspices of Turkey and Russia, a new government was formed. With Assad gone, the US and the EU revoked most sanctions, and Syria re-embarked on its long road back to normalcy. The worst had been avoided.

CHAPTER 15

IRAN'S CODE REVOLUTION

The fight for human cyber rights

by
PATRYK PAWLAK

Assumptions 2030

- Digital authoritarianism continues to rise
- Defence of human rights turns assertive
- Conflicts play out on- and offline

Hashem Mohammadi arrived at his post at the Computer Emergency Response Team of Iran (CERTCC MAHER) much earlier than normally. He did not expect that in just a couple of hours his computer screen and the workstation at which he usually enjoyed Koluche cookies and coffee would become the frontline in the confrontation between Iran and the Global Coalition for Defence of Democracy (GCDD).

At 9.00 am, the US Cyber Command – in coordination with other members of the GCDD, including Australia, Canada, the United Kingdom and several European members of NATO – conducted a cyberattack against several targets in Iran, including the state-owned media and most importantly the Islamic Revolutionary Guard Corps (IRGC). A day earlier, the European Union had imposed human rights sanctions on members of the hardline Guardian Council and the IRGC in response to Iran's continued violations of several UN Security Council resolutions, increased internet shutdowns, and the controversial decision to execute five journalists and bloggers whose activities were deemed prejudicial to the regime. For the first time, the EU's 'Magnitsky Act' adopted almost 10 years earlier, was used to impose sanctions for the violations of human rights online.

What nobody knew at that time is that that morning of 10 December 2030 would open a new chapter in the history of conflicts – one that historians and analysts will later describe as the 'Code Revolution' with a new vocabulary featuring terms such as 'digital ethnic cleansing', 'humanitarian cyber intervention' or 'responsibility to hack'. Its main casualty: human rights online.

...

It all started rather innocently. In the early 2020s, the world got rather used to a tit-for-tat exchange between the United States and Iran whereby operations against the elements of each other's critical infrastructure become the new normal in their bilateral relations. While most of the international political capital was devoted to preserving the nuclear deal with Iran, Tehran's increasingly blatant disrespect for human rights online was becoming difficult to accept.

But the rise of 'digital authoritarianism'[1] was not just the 'Iran problem'. The speed of the digital transition and the reliance on new technologies in many countries around the world has outpaced reforms that would provide adequate safeguards for citizens. Between 2019 and 2025, the number of internet shutdowns around the world had increased from 213 across 33 countries to 530 instances in 93 countries. That means that by 2025 the majority of countries around the world had imposed limitations on access to the internet.[2] The growing powers of the big tech companies and the lack of transparency have ultimately let some to conclude that the 2020s have marked the age of 'digital slavery'[3] and 'algocracy.'[4] Consequently, the protection of human rights online has gradually weakened around the globe, fuelling the already apparent conflict between the liberal democracies and alternative models of governing.

1 Adrian Shabaz, "The Rise of Digital Authoritarianism", Freedom House, October 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

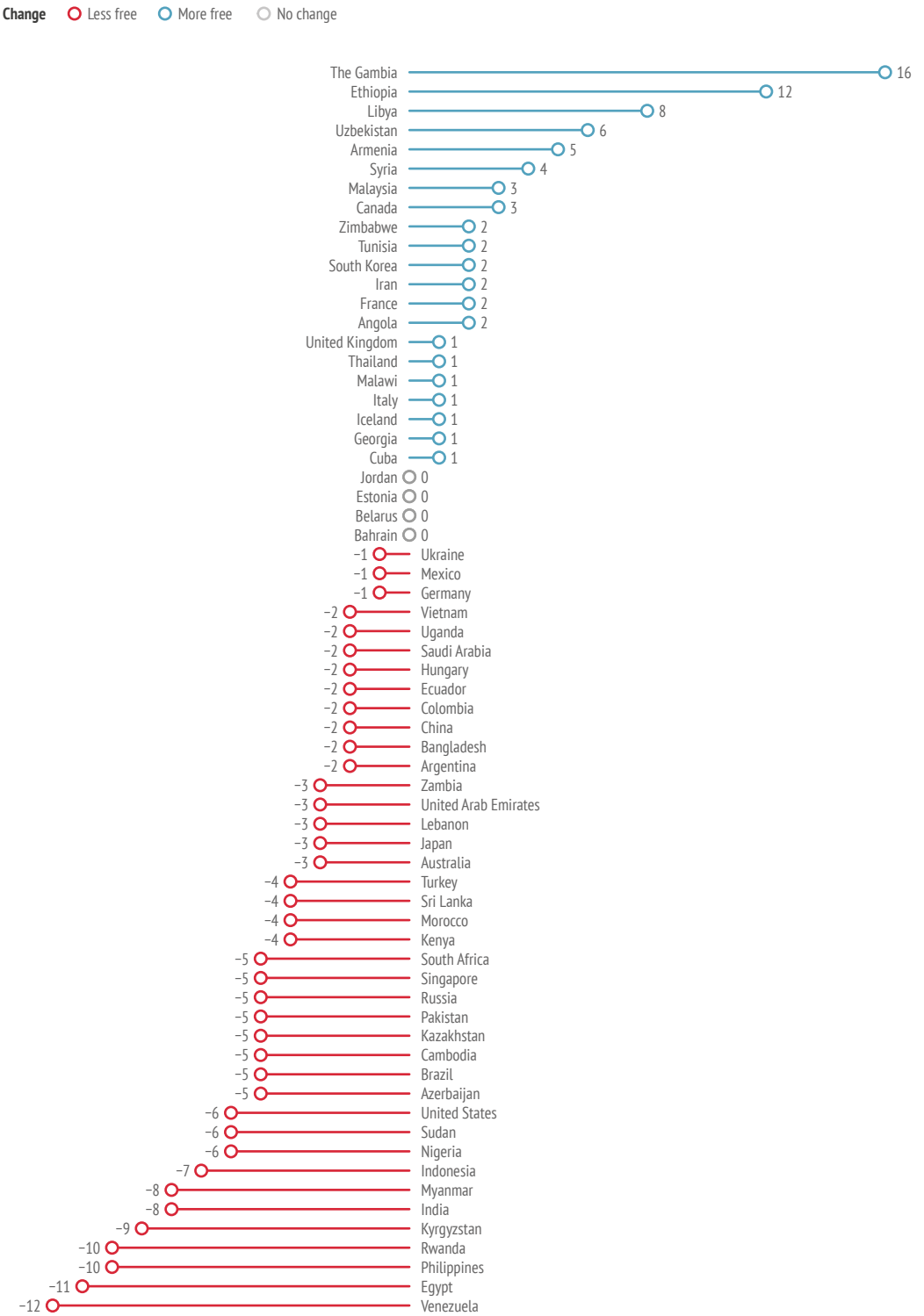
2 "How internet shutdowns are affecting 2020 elections, and what you can do about it", *accessnow*, 2020, https://www.accessnow.org/keepiton/

3 Mick Chisnall, "Digital Slavery: Time for Abolition?", *Policy Studies*, vol. 41, no.5, 2020, https://www.tandfonline.com/doi/abs/10.1080/01442872.2020.1724926?journalCode=cpos20

4 https://link.springer.com/article/10.1007/s13347-015-0211-1

Internet freedom

Freedom of the Net score, 5 year change, 2016–2020



Data: Freedom House 2016; Freedom House 2020

Iran was not an exception, but it definitely ranked as the frontrunner when it came to the violation of human rights online. A perfect storm came about in 2024 during the elections for the new Assembly of Experts. The stakes were high given that its newly elected members would also be the ones appointing the next Supreme Leader of Iran, following the death of Ali Khamanei. As the moderate clerics were expected to defeat hardliners, the Guardian Council who vet the candidates disqualified more than 3,600 reformist and independent candidates, including all women.

Iranian society responded with widespread protests across the country with social media used as the primary tool for mass mobilisation. Reformists gathered around the former President Mohammad Khatami accused the Council of 'threatening Iranian democracy' by favouring candidates close to the IRGC and consequently ensuring their influence over the political, economic and cultural life of Iran. This was the scenario that the regime was preparing for and so the response was swift. Since 2015, the IRGC had been conducting a regular military exercise dubbed 'Eghtedare Sarallah' and developed an efficient machinery that allowed for the monitoring of social media activities and offensive cyber operations against domestic and foreign targets. When the protests erupted, the head of the Iranian Cyber Police (FATA) quickly declared a zero-tolerance policy for any acts aimed at undermining public order ahead of the elections.

The digital footprint of the IRGC had only grown and its efforts to control online content and activities within its territory had intensified. The development of SHOMA - Iran's intranet - and the state's control over the internet backbone provided the government with the ability to throttle foreign connection speeds during the anti-government protests organised by the Gonabadi Dervishes. The final blow came with the imposition of the death sentence on five pro-reformist writers and editors with 20 more sentenced to 12 years in prison on the grounds that their actions damaged 'public morality' or resulted in the 'dissemination of lies'.

Responding to the developments in Iran, the European Council in December 2024 stated that "this continued assault on human rights and dignity cannot be tolerated". Recalling the Human Rights Council Resolution on the Protection of Human Rights Online adopted in September 2023 by a narrow majority of votes (despite the efforts by members like China, Cuba, Pakistan, Russia and Uzbekistan), European leaders recalled the importance of a "free, open and safe cyberspace" for growth and international security and called upon Iran to stop the violations. The language adopted by the EU was a careful attempt to preserve the already fragile nuclear deal with Iran. Nonetheless, the EU also decided to forbid any trade in technology that might be used to limit civil liberties in Iran. Consequently, several companies were asked to default on their pre-existing contractual obligations in Iran – such as Nokia who had signed an agreement with Iran for research and delivery of 5G mobile service and whose clients included fixed-line operator HiWeb, mobile operator MTN Irancell, and the Mobile Communications Company of Iran. Other members of the GCDD established in 2021 to "promote and protect the integrity of democratic institutions online and offline" – of which human rights online were considered a key component – took equally decisive steps, including a new round of human rights sanctions.

But these moves only emboldened hardliners in Iran who tightened control over any secular and anti-government content. By 2026, any information about the Dervish minority disappeared from the Iranian internet. It was deemed illegal as contradicting state doctrine regarding Islam. At the same time, any reporting about the Dervish minority was forbidden on the grounds of "disturbing public order" and spreading "propaganda against the state". The Telecommunications Company of Iran (TCI) – with the IRGC as majority stakeholder –- retained a monopoly on internet traffic flowing in and out of the country and its dominance of the ISP market offered all necessary means for the security apparatus to monitor online activities. The Committee to Determine Instances of Criminal Content (CDICC) - a government body headed by the Prosecutor General consisting of representatives from 12 state institutions

– further strengthened the enforcement of the ban on the most prominent social media platforms such as Facebook, Twitter, YouTube, Instagram and Telegram.

In a campaign spearheaded by Human Rights Watch, Access Now and International Crisis Group, a coalition of over 100 human rights groups described Iran's actions as "a government-sanctioned campaign of digital ethnic cleansing" that requires a firm response from the international community. Listing numerous online abuses and violations of international law scrupulously documented by the Centre for Human Rights in Iran, the letter called for the states to develop a new doctrine of "humanitarian cyber intervention" and "responsibility to hack" as the only mechanisms that will protect millions of people against the new forms of abuses available to states in the digital age.

Subsequent media reports have revealed that the organisations went further than just the letter: Human Rights Watch in cooperation with pro-human rights hacktivist groups orchestrated a cyberattack against the network of the Interior Ministry that destroyed data on 5,000 computers, deleting a database containing information about reformist journalists, activists and religious minorities. In retaliation, the Iranian Ashiyane Digital Security Team, previously known for hacking websites and replacing their home pages with pro-Iranian content, retaliated with attacks against the organisations who signed the letter and the media outlets who circulated it on their websites. In a hack-and-leak operation, the ADST gained access to a database of over 10,000 human rights defenders based in 35 countries and published it, thereby putting their lives in direct danger.

...

The 'Code Revolution' of 2030 has resulted in the intensified use of cyber operations and the conflict over compliance with human rights regimes has taken on new dimensions. As a direct result of the EU and US policies regarding the sale of technologies to Iran, the IRGC pursued its own version of digital sovereignty and decided to replace all Western technology within its internet infrastructures with digital solutions offered by China. This was accompanied by an extensive use of new technologies that relied on artificial intelligence to identify and target anti-regime voices as well as to remove the content deemed prejudicial to the regime. The IRGC also stepped up its reliance on trusted intermediaries to manage contracts with independent hacker groups to conduct harassment campaigns aimed at targets in the West.

Ultimately, two major developments marked the aftermath of this conflict. First, the GCDD has embraced a doctrine of "humanitarian cyber intervention" with the "responsibility to hack" at its core. The doctrine aims to prevent a state from acting against its population and jeopardising their welfare through repression, violence and exposure to mistreatment using online tools. Second, this new type of conflict brought to the fore the important role that non-state actors play during cyber conflicts. By 2032 Elon Musk's Starlink satellites provided universal access to the internet which deprived authoritarian regimes of the ultimate tool of control and oppression. The same year Musk received the Sakharov Prize awarded by the European Parliament.

POLICY CONSIDERATIONS

Conflict in the age of lost innocence

by
SIMONA R. SOARE

The world has lost its innocence *again* by 2030. This is the implicit conclusion of the 15 scenarios in this *Chaillot Paper*. Conflict is pervasive and inherent across different sectors of activity, domains of warfare and regions of the world. The distinction between traditional concepts of 'war' and 'peace', 'conflict' and 'warfare', 'internal' and 'external' security has become superfluous. Political interests are factionalised within and across borders as the state is increasingly challenged by new manifestations of conflict yet remains indispensable to confront them. Ubiquitous technological innovation, accelerated by 5G and artificial intelligence (AI), is a significant variable of the future of conflict,[1], but it does not predetermine it. Rather, the element of continuity, notably the centrality of human political interests and identity – accentuated and accelerated by the diffusion of power from states to other types of actors – is the main driver that shapes the evolution of conflict in the future. This leads to a growing hybridisation of conflict and a universalisation of the battlespace, used here comprehensively rather than with an exclusively military meaning, as well as to an uncomfortable tendency towards the progressive securitisation of every aspect of society, be it domestic or international.

What implications could the scenarios in this volume – or similar future events – carry for policymaking? How can Europeans best equip themselves to efficiently navigate future conflicts? In what follows policy considerations derived from the scenarios in this *Chaillot Paper* are broken down into seven interlinked categories.

SITUATIONAL AWARENESS AND PREDICTION CAPACITY

To ensure European states are ready to tackle increasingly hybrid and complex risks and threats and to ensure they can effectively implement the comprehensive approach to conflict, they need a *reliable and comprehensive situational awareness, understanding and prediction* capacity. The EU's Strategic Compass – and its successor strategies – should lay the foundations for such a capability to be developed and implemented. This capability can be achieved through the development and implementation of an enhanced common early warning and indicators system which would facilitate the monitoring and understanding of specific security threats. The goal would not be solely

1 Raphael S. Cohen *et.al,* "The Future of Warfare in 2030: Project Overview and Conclusions" RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR2849z1.html.

the early detection of new security challenges, but rather the mapping and understanding of their evolution over time and space, especially along the internal-external nexus; the early identification of conflict trigger factors to minimise surprise and identify geopolitical pressure points; and early conflict mapping for a better predictive understanding of how the conflict could evolve, including how it might internationalise. For example, an AI-enabled EU strategic dashboard could be developed as an interface to monitor in real time evolutions on the ground in key states and areas and assist rapid decision-making with respect to the deployment of different available tools and resources, depending on the stage of escalation and/or de-escalation in which the conflict finds itself.

European states already have a good track record on developing early warning indicators for crises and conflicts, counterterrorism, counter-piracy and hybrid threats which could be built upon and adapted. And technological progress enables their refinement and adaptation. For example, law enforcement authorities in some countries are using AI to fuse data from various sources to map out networks and patterns in counterterrorism, to counter organised crime and violent extremism operations.[2] Technical and governance challenges exist – such as over data sharing and use – requiring a concerted EU and NATO effort to solve them.

Ubiquitous technological innovation is a significant variable of the future of conflict, but it does not predetermine it.

PLANNING AND PREPAREDNESS

Preparedness and planning are necessary components of any EU-wide strategy and, where appropriate, in conjunction with NATO collective strategies, are essential to build resilience, enhance deterrence and exercise effective defence. In this context, both *E*U threat assessment and security strategy development should be institutionalised, performed regularly and aligned with changes in European political leadership. Furthermore, such an effort should strive to better align and integrate the European normative approach, with its economic and trade policy and with its security and defence policy. As automation, big data analytics and AI will exponentially reduce decision-making time and space for political debate, three aspects are increasingly important for building resilience and enhancing deterrence.

The first is that Europeans need to *develop and exercise regularly multiple conflict and crisis scenarios*. This will help identify and map out early the vulnerabilities and gaps in their planning and preparedness and may even lead to a regular and honest *vulnerability mapping exercise* as the basis of developing the resilience of European governance, institutions, supply chains and society more broadly. Hybrid threats and disinformation, but also a number of external threats with domestic manifestations, exploit known or unknown vulnerabilities in European societies. Shedding light on these vulnerabilities, be it in the governmental or private sector, at the national or local levels, helps increase resilience as well as eliminates avenues of conflict diffusion within European societies. Readily available tools exist,

2 Alexander Stamos, Written Testimony on "Artificial Intelligence and Counterterrorism: Possibilities and Limitations" before the US House of Representatives Committee on Homeland Security, June 25, 2019; Brian Fishman, "Crossroads: Counter-terrorism and the Internet" *Texas National Security Review*, vol. 2, no. 2 (February 2019): https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/; Damon Paulo et al, "Social Network Intelligence Analysis to Combat Street Gang Violence", Cornell University Press, June 2013, https://arxiv.org/abs/1306.6834.

particularly foresight scenario planning, the integration of foresight and forecasting tools,[3] or a combination of the two with modelling and simulation. Building on existing EU and NATO exercises, such efforts should be extended and replicated at lower decision-making levels (e.g. local governance) and should be developed based on an inclusive multi-stakeholder approach.

The second element is the need to ensure European states develop a *coherent joint civilian-military capability assessment*, in relation to the identified clusters of crisis and conflict scenarios, so as to have a comprehensive image of the assets and power levers European states have available to deploy in any given context. The Common Security and Defence Policy (CSDP) Civilian Compact is a good start. However, such planning should be extended and be more ambitious in terms of the capabilities and assets it can draw on and more integrated with the parallel military capability assessment process. For example, AI-enabled modelling and simulation can become an asset by helping European states to simulate the application of multiple mixes of instruments and tools in specific scenarios, at different stages of crisis or conflict, to better determine their effectiveness, lay out the most efficient available options and assist with rapid decision-making.[4]

European states already have a good track record on developing early warning indicators for crises and conflicts.

The last element is the *alignment between European agreed interests, enhanced situational awareness and decision-making*. This may potentially require a reassessment of European individual and collective threat/risk tolerance benchmarks and thresholds for (early/preventive) action. External conflicts that have greater chances of domestic manifestations in one or more European states, may require more preventive action than currently assumed and practised. As no European state will foreseeably possess sufficient resources and capabilities to act unilaterally in a future contingency, a reassessment of European-level decision-making procedures – such as, but not limited to Qualified Majority Voting (QMV)[5] – will be necessary while also keeping in mind the need to maintain as broad a legitimacy for European actions and measures as possible. After all, efficient action in EU foreign and security policy should enhance, not come at the cost of, European political solidarity. In addition, the *adaptation of legal and bureaucratic governance structures*, not least through the adaptation and/or adoption of new legal powers to act at lower decision-making levels, in the civilian and military domains alike, may also be required. These include back office processes, such as acquisitions and personnel management, but they also entail battlefield rules of engagement particularly involving the use of unmanned military force.

POSTURE, CONCEPTS AND CAPABILITIES

The future of conflict is multi-domain[6] and it will be increasingly difficult to predict which domains of warfare will offer decisive strategic advantages. Consequently, *Europeans will have*

3 J. Peter Scoblic and Philip E. Tetlock, "A Better Crystal Ball: The Right Way to Think About the Future" *Foreign Affairs,* vol. 99, no. 6 (November/December 2020): pp. 10-19.

4 See, for example, work on simulation-based decision making in a military environment developed by the NATO Science and Technology Organization, "Data Farming Services for Analysis and Simulation-Based Decision Support," May 20, 2020, https://www.sto.nato.int/Pages/technical-team.aspx?k=%28%2A%29&s=Search%20MSG%20Activities.

5 Ursula von der Leyen, "State of the Union Address by President von der Leyen at the European Parliament Plenary", Brussels, September 16, 2020, https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_20_1655.

6 NATO Allied Command Transformation, "Innovation Hub Warfighting 2040 Project Report: How Will NATO Have to Compete in the Future?" Norfolk, Virginia, March 2020, https://www.innovationhub-act.org/sites/default/files/2020-06/WF2040Report.pdf.

to master all domains for deterrence, defence, warfighting and crisis management purposes. The prevalence of lower intensity conflicts among the scenarios in this volume suggests the military instrument may be one of many tools of power required to tackle future conflicts, but by no means the dominant one as in the past. Indeed, in few of the scenarios would European military intervention be necessary. However, this highlights *t*he need for European states to rapidly develop their collective ability for cross-domain coercion by becoming more agile in terms of the synergistic application of different instruments of power, at different governance levels (e.g. national, European, transatlantic) to achieve desirable strategic effects.

Furthermore, European states need to develop their military capabilities to be ready to face future conflicts. This entails three elements. The first is to develop as a matter of urgency the right mix of modern *military capabilities* to sustain a larger, high-readiness, well-trained, multi-domain full-spectrum force package – the kind needed to project power over long distances and extended time horizons, including in high-intensity multi-domain warfare. The second is to develop and train for a European *military doctrine* and *common strategic culture* that informs the operational employment of European armed forces. Finally, the last element refers to the development of a European *force posture* that enables Europeans to rapidly respond to a variety of contingencies regionally and globally.

Perhaps unsurprisingly, the scenarios in this volume feature geopolitics and great power competition quite centrally, but *the dominant concern is with the evolution of conflict in relations with Russia rather than with China.* This highlights the continued relevance of NATO in enhancing collective defence and EU-NATO cooperation in supporting it. However, European ability to defend interests in the Arctic, Eastern Europe, the Indo-Pacific and on the African continent depends on significantly more European power projection capabilities, especially in the air and maritime domains, including through a range of manned and unmanned, autonomous military platforms as well as conventional capabilities. Most of the capabilities required to tackle future conflict feature front and centre in the Capability Development Plan (CDP), among the priorities identified in the 2020 Coordinated Annual Review on Defence (CARD) Report[7] and among ongoing Permanent Structured Cooperation (PESCO) projects or announced future joint endeavours. Within a time horizon of ten years, the development of these capabilities, in sufficient numbers and complemented by enhanced training and upgraded dual-use and military critical infrastructure, would better position European states for the types of conflicts described here.

However, even developing the required military capabilities will not erase all dependency on and need to work together with allies and partners. Consequently, *updated contingency planning is needed for multilateral operations involving European as well as non-European/EU allies and partners*. To operate globally, Europeans also need to be better positioned globally, be it to defend their interests and values regionally or to defend the global commons and preserve the rules-based international order. This entails a larger European military footprint and a European/EU developed network of security partnerships especially in areas where Europeans expect they are more likely to use military force in the future. These can be achieved through enhanced investments in closer military-to-military relations, partner capacity-building efforts, closer capability development, joint training and exercises, foreign military sales and greater military interoperability and intelligence cooperation with partners in other regions.

7 See European Defence Agency, "2020 CARD Report: Executive Summary", November 23, 2020, https://www.eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf; European Defence Agency, "Exploring Europe's capability requirements for 2035 and beyond", June 2018, https://www.eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf.

DEFENCE AS ROUTINE

As many of the scenarios in this volume show, future conflict could be driven by politically motivated violence, deeply influenced by context and based on social grievances about political, technological and other types of governance, but it may not necessarily be politically (state or non-state) directed. Enabled by rapid technological progress and proliferation, potential adversaries will have access to more vectors of attack – short of high-intensity war (to which there is considerably less reference in the scenarios) – and will be more loosely networked.

However, to defend their interests and their security as well as to contribute to global peace and security, European states' defensive measures are inherently defending not a specific battlefield, but their societies more generally. A country's economy and society cannot grind to a halt or shift focus to defend against a cyberattack or even a pandemic. Increasing urbanisation and connectivity makes urban spaces particularly easy targets for external and domestic foes, which significantly complicates response measures. But smart city infrastructure is rapidly expanding in Europe, and, with it, so also is the increasing risk of disruption through malign cyber and hybrid tools. Consequently, building resilience, deterrence and, if all else fails, implementing defence has to become less disruptive to normal societal activities. And European and transatlantic strategies to build resilience, enhance deterrence and consolidate defence have to be reassessed with this in mind. As such, European states will have to be in the business of defence as a routine service while also delivering governance and providing a growing range of social services at higher standards.

European states' defensive measures are inherently defending not a specific battlefield, but their societies more generally.

STRATEGIC COMMUNICATIONS AND MESSAGING

The scenarios in this *Chaillot Paper* paint the picture of a conflict that evolves out of social grievances about national and international governance in the physical and virtual domains. These grievances simultaneously include a sense of social injustice and socio-economic inequality – feeding left-wing political movements; a sense of governance inefficiency and lack of policy ethics – feeding different anarchist manifestations; and a sense of overwhelming loss of identity, tradition and *self* – feeding right-wing and conservative movements. Of course, many of these elements are not new, as evidenced by the struggle against radicalisation and violent extremism. However, in contrast to the twentieth century, the future of conflict seems less about an ideological struggle for the absolute victory of a political governance model and more about the factionalisation of the political dynamics of conflict that do not compete but co-exist within national territories and transnationally.

In other words, political dynamics within Europe and beyond its borders will increasingly shape European responses to future conflicts. To prevail in future conflicts, technological and informational superiority will be important, but ultimately the battle will be won in the hearts and minds of the people, in Europe *and* elsewhere. If the human mind is to become the 'battlefield' of future conflicts, then effective communication should be an essential part of the European toolkit for tackling conflicts and for building effective societal resilience.

This puts a premium on an effective European *strategic communications* and *messaging capacity*, particularly tailoring governance to respond to both narratives on the right and the left sides of the political spectrum and to defeat populist

and nationalist tendencies. Speaking with one European voice will be important, but more important will be the actual messaging that comes out of European capitals and how coordinated it is. *How and when Europeans communicate about different future conflicts may become as important as how they concretely act to contain and resolve them*. It will thus be particularly challenging and crucial in the context of such new political dynamics of conflict to *maintain European solidarity*. To succeed, European strategic communications and messaging needs to be underpinned by a solid perspective of and political commitment to the future of European democracy, economic prosperity and rule of law as much as to multilateralism and the rules-based international order.

CONVENING POWER

Another striking feature about the trends in future conflicts described in this volume is not the European proclivity or need to act autonomously, but rather a continued need for European states to navigate different layers and levels of security and defence governance in Europe and in relation to transatlantic allies and partners, through multiple formats and platforms – EU-US, EU-NATO, NATO, CSDP, the European Intervention Initiative (EI2) and other regional groupings.

Proficiency and agility in navigating the complex layers of security governance in Europe will be necessary for European states to effectively tackle future conflicts. Importantly, this suggests that Europeans should invest more in developing Europe's convening power, its ability to deploy diplomatic and economic tools to shape international outcomes but also its ability to build security and defence coalitions when need arises. Clarifications regarding the EU's security and defence governance policy, the adaptation of NATO and the prospects of improved EU-NATO cooperation, as well as the agreement of an Anglo-European security cooperation framework are necessary steps in the right direction. Further efforts at explaining the underpinnings of articles 42(7) TEU and 222 TFEU, particularly in view of enhancing EU-NATO synergies, are also necessary. But if work in these areas does not pick up pace, Europe will be less, not more, prepared to tackle future conflicts by 2030.

SMART BUDGETING AND THE POWER OF INNOVATION

A significant implication of tackling future conflict is *cost*. Now more than ever, European states need to be more self-reliant in security and defence,[8] but defence is not cheap and effective defence cannot come at the cost of European overall solvency.[9] Across Europe, defence budgets have steadily increased over the last five years[10] but, looking ahead, the sustainability of the defence budgets required to tackle future conflicts is anything but assured. Sustained simultaneous investment in technological innovation, diplomacy and multilateralism, military capabilities and strategic communications, development and more will be required under growing economic challenges stemming from the erosion of Western economic power. This suggests

Defence is not cheap and effective defence cannot come at the cost of European overall solvency.

8 Jiří Šedivý, "Now, more than ever" *European Defence Matters*, no. 19, 2020, pp. 4-6.

9 Robert Murray, "Building a resilient innovation pipeline for the Alliance" *NATO Review*, September 1, 2020.

10 NATO, "Defence Expenditure of NATO Countries (2013-2020)" *Press Release*, October 21, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/10/pdf/pr-2020-104-en.pdf; European Defence Agency, "Defence Data 2017-2018: Key Findings and Analysis", 2019, https://www.eda.europa.eu/docs/default-source/brochures/eda-defence-data-2017-2018.

a continued and growing added value of Europe (i.e. the EU) in facilitating and incentivising European cooperation and, if need be, pooling and sharing of resources to maximise their strategic impact. In light of growing economic and budgetary pressures, harnessing the power of innovation across the societal, industrial, economic and military spectrum will increasingly become indispensable. This puts in perspective the concepts of strategic autonomy or technological sovereignty as well as, equally important, the *avoidance and/or reduction of the fragmentation of European investment in innovation* across all these distinct but interrelated domains.

A CONCLUDING THOUGHT

The quality and the ability of the scenarios in this volume to bring out trends in the future of conflict is undeniable. Nevertheless, it is worth considering as Europeans prepare for the future of conflict that the view expressed in this volume is complementary to similar projections in other regions of the world, without being by any means the prevalent perspective on the future of conflict. So, a serious dose of adaptability, flexibility in approaching the future of conflict and a sense of proactive prevention and mitigation is highly recommended.

While the scenarios in this *Chaillot Paper* highlight gaps in capabilities, power attributes or geographical focus for European states' ability to tackle future conflicts, what is perhaps surprising in these texts is that there is also a strong sense of validation and even confirmation of the current trajectory upon which Europe has embarked as the solution to such future conflicts – more multilateralism, more defence cooperation, a more proactive European role on the world stage, more technological and defence innovation. In short, *the key for Europeans to be prepared for the future of conflict is more Europe, done better.*

ABBREVIATIONS

A2/AD
Anti-Access/Area Denial

AI
Artificial Intelligence

BRI
Belt and Road Initiative

CEO
Chief Executive Officer

CPL
Congolese Party of Labour

CSDP
Common Security and Defence Policy

DOD
Department of Defense

GCDD
Global Coalition for the Defence of Democracy

GDP
Gross domestic product

GRU
Russian military intelligence agency (*Glavnoye Razvedyvatelnoye Upravlenie*)

IRGC
Islamic Revolutionary Guards Corps

IS
Islamic State

ISP
Internet service provider

IT
Information Technology

JCPOA
Joint Comprehensive Plan of Action

NATO
North Atlantic Treaty Organisation

NGO
Non-Governmental Organisation

PLA
People's Liberation Army

PLAN
People's Liberation Army Navy

PRC
People's Republic of China

R&D
Research and Development

S&T
Science and Technology

SOF
Special Operations Forces

STANAG
Standardisation Agreement

TEU
Treaty on European Union

TFEU
Treaty on the Functioning of the European Union

UNCLOS
United Nations Convention on the Law of the Sea

UPADS
Pan-African Union for Social Democracy

USMC
United States Marine Corps

UUV
Unmanned underwater vehicle

VR
Virtual Reality

WCO
World Customs Organisation

NOTES ON THE CONTRIBUTORS

Natasha E. Bajema is a national security expert, founder and CEO of Nuclear Spin Cycle, and a fiction author. In her work she specialises in weapons of mass destruction (WMD), nuclear proliferation, terrorism, and emerging technologies. Previously she worked for the National Defense University advising senior leaders at the Pentagon and teaching a course on WMD and film.

Lotje Boswinkel is Strategic Analyst at the Hague Centre for Strategic Studies (HCSS). Previously she worked as a trainee at the EUISS on the Middle East and North Africa, the geopolitical impact of Covid-19, and the future of warfare. She has co-authored various policy briefs and chapters in publications.

Ali Fathollah-Nejad is a political scientist working on Iran, the Middle East, the post-unipolar world order, and right-wing populism in Europe. He is Affiliated Researcher at the Centre d'Études de la Coopération Internationale et du Développement (CECID), the Université libre de Bruxelles (ULB), and the Center for Middle Eastern and North African Politics, Freie Universität (FU) Berlin.

Daniel Fiott is Security and Defence Editor at the EUISS. He analyses European defence policy, CSDP, defence capability and industrial issues and hybrid threats. He is the Institute's representative to the Executive Academic Board of the European Security and Defence College (ESDC) and the author of the Institute's annual *Yearbook of European Security*.

Franz-Stefan Gady is Research Fellow for Cyber, Space and Future Conflict at the International Institute for Strategic Studies (IISS), and a columnist for *The Diplomat.* He is the author of a number of monographs and book chapters on Asian and European security issues, and has advised militaries in Europe and the US on structural reform and the future of conflict.

Florence Gaub is Deputy Director at the EUISS, where she is in charge of coordinating research activities. In addition, she works on strategic foresight, as well as security and conflict in the Middle East and North Africa. She has published widely and testifies regularly at governmental and parliamentary hearings. Previously, she worked at NATO Defence College.

Zoe Lockman-Stanley is Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S Rajaratnam School of International Studies in Singapore. Her research focuses on defence innovation, security-related emerging technologies, defence industries, and military capability development.

Kathleen J. McInnis analyses international security and defence issues for the United States Congress. Her areas of expertise include US global basing and posture, Asian and European alliance dynamics, nuclear strategy, military coalitions, counterinsurgency, and Afghanistan. She is a novelist and has worked in the Pentagon, the UK Parliament, and in think tanks on both sides of the Atlantic.

Nicolas Minvielle specialises in innovation and design. He is head of the master's degree programme in Design, Marketing and Creation at the Audencia Business School in Nantes, and cofounder of the design fiction collective *Making Tomorrow*. He is also facilitator for the French Army's 'Red Team' of science fiction writers helping military strategists to anticipate future threats to national security. He is

co-author of the blog *imaginaries-at-work.com*, and has written various books.

Andrew Monaghan is Director of the Russia Research Network, Ltd. He is also Senior Associate Fellow at the Royal United Services Institute (RUSI) in London, and a Non-Resident Associate Fellow of the NATO Defence College in Rome. He is the author of *Dealing with the Russians* (Polity, 2019) and *Power in Modern Russia* (MUP, 2017).

Katariina Mustasilta is a Senior Associate Analyst dealing with conflict research at the EUISS. Her research applies both quantitative and qualitative methods to study the drivers of countries' internal conflicts and how to prevent violent escalation, the dynamics of civil resistance, and local peace and conflict dynamics. She is the editor of the EUISS Conflict Series.

Patryk Pawlak is the EUISS Brussels Executive Officer. In this capacity, he maintains and develops relations with other Brussels-based institutions. In addition, he is in charge of the cyber portfolio, leading the Institute's cyber-related projects and contributing to its outreach activities. Since June 2016, he has been a member of the Advisory Board of the Global Forum on Cyber Expertise.

Tobias Pietz is Deputy Head of the Analysis Division at the Center for International Peace Operations (ZIF). His main areas of work are CSDP missions, peacekeeping partnerships and cross-cutting issues such as gender, migration and climate security. Previously, he worked at the Bonn International Center for Conversion (BICC) on small arms control and demobilisation of former combatants.

Sinikukka Saari is a Senior Associate Analyst at the EUISS working on Russia, the Eastern Partnership countries and Central Asia. Previously, she worked at the Policy Planning and Research Unit of the Ministry for Foreign Affairs of Finland, at the Mission Analytical Capability Unit of the European Union Monitoring Mission (EUMM) in Georgia, and in the Russia and Eastern Neighbourhood Programme at the Finnish Institute of International Affairs.

Stanislav Secrieru is a Senior Analyst at the EUISS covering Russia and the EU's eastern neighbourhood. His research interests focus on EU-Russia relations, Russia's foreign and security policy in the post-Soviet region, protracted conflicts, and the EU's relations with the Eastern Partnership states.

Simona R. Soare is a Senior Associate Analyst at the EUISS, where her research focuses on transatlantic and European security and defence, EU-NATO cooperation and defence innovation. Prior to joining the EUISS, she served as advisor to the Vice-President of the European Parliament, as analyst with the Romanian Ministry of Defence and she has been a lecturer in international security. She is also a Department of State Fellow in US foreign, security and defence policy.

Bruno Tertrais is Deputy Director at the Fondation pour la recherche stratégique (FRS), and Senior Fellow at the Institut Montaigne. He has published widely on international relations and geopolitics, conflict, US strategy, transatlantic relations, security in the Middle East and Asia, nuclear proliferation and deterrence, and military strategy.

Olivier Wathelet is an anthropologist (PhD) with a strong interest in cultural dynamics and innovation. He runs *Users Matter*, a small research agency with a user-centric design approach. He is co-founder of the design fiction collective *Making Tomorrow* and writes frequently on how to better link anthropology, forecasting and design.

"History is littered with mistaken predictions about the future of warfare": taking this observation as its premise, this *Chaillot Paper* takes a novel approach to exploring how future conflicts might unfold.

In contrast to traditional schools of conflict anticipation, which rely on science, history and deduction, it combines imagination with an analysis of past and present trends to paint a compelling picture of conflicts to come. This approach, which incorporates elements and tools drawn from science fiction and futuristic art and literature, also takes account of hitherto unknown factors and drivers of conflict – new technological developments, environmental changes, or ideologies yet to be born.

The volume presents 15 fictionalised scenarios that imagine how future conflicts might occur. These scenarios contribute to, and at times challenge, the existing body of assumptions concerning the genesis of conflict, its likelihood and how it might play out. Reflecting the creative and collaborative spirit that underlies this publication, the authors who devised these scenarios embarked on a truly innovative project taking them out of their comfort zone and into the realm of foresight.

EUISS EUROPEAN UNION Institute for Security Studies

Publications Office of the European Union

ISBN 978-92-9198-973-7
CATALOGUE NUMBER QN-AA-20-005-EN-C