INTERNATIONAL SECURITY FORUM BONN 2019

Full Report
Rapporteur: Simone Becker

FORUM REPORT

COMMENTS AND PERSPECTIVES

Dear readers,

After the enormous optimism following the fall of the Berlin Wall, the world looks a lot less clear-cut than it did around the turn of the millennium. From the effects of climate change, new challenges in the global management of the sea, space, and cyberspace, and escalating instability in some of the world's most vulnerable regions, it appears that global challenges are mounting at the same rate as tensions between states are rising.

Academia isn't meant to be an ivory tower, but needs to help provide a solid foundation for political decision-making to crucial political and societal challenges. The University of Bonn is attempting to contribute its part. Establishing the *Center for International Security and Governance (CISG)* in 2014, led by Prof. James D. Bindenagel, was one sign of this. Now, the university is building on its past accomplishments and expanding its existing expertise into a new structure. Because of this, the 2019 International Security Forum marked a special occasion: On October 1, 2019, we celebrated the inauguration of a new interdisciplinary research body – the *Center for Advanced Security, Strategic and Integration Studies (CASSIS)*, an innovative research structure that combines security and strategic studies with European integration research, while closely linking academic theory and political practice.

As this new institution is gaining momentum, we would like to thank those who have made this possible: The University of Bonn and its Rector, whose foresight and dedication have lifted our alma mater into the ranks of Germany's elite "Universities of Excellence" in 2019; and Prof. Dr. Volker Kronenberg, Dean of the University's Faculty of Arts, for his key role in establishing CASSIS.

In view of the enormous complexity that marks our world, the path forward is not always clear, and solutions to complex issues are rarely simple. That's why sound academic research and a thorough knowledge of the challenges at hand need to be accompanied by careful consideration and an openness to different, heterodox perspectives. It's also why formats such as the International Security Forum are so important. The Forum is a platform for open international discussions and a place for "constructive exchange to come to a new understanding", as AICGS' Jeffrey Rathke recently put it so aptly.

The report you have before you is dedicated to providing an insight into the 2019 International Security Forum and offers a glimpse into current debates on some of the most pressing foreign and security policy issues. In its last section, some of the Forum's experts and policymakers also share their unique take on some of this year's issues through personal comments. We hope that this collection of views and perspectives will provide you with some deeper insights!

CASSIS and AICGS would like to extend our special thanks to all participants as well as our partners and supporters: the Konrad Adenauer Foundation, the German Council on Foreign Relations (DGAP), the U.S. Consulate General Düsseldorf, the City of Bonn and the Cyber Security Cluster e.V., as well as NRW Secretary of State Dr. Mark Speich, former PM of NRW Prof. Dr. Jürgen Rüttgers, and Dr. Peter Fischer-Bollin.

We look forward to hosting new debates shortly. Happy reading!

Dr. Enrico Fels
Managing Director of the Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn

Prof. Dr. Wolfram Hilz
Professor for Political Science and Acting Director of the Center for Advanced Security, Strategic and Integration Studies, University of Bonn

Participants of the International Security Forum Bonn 2019

Prof. Dr. Volker Kronenberg and Prof. James D. Bindenagel, both University of Bonn, with Jeffrey Rathke, AICGS

*We can't solve problems by using the same
kind of thinking we used when we created them.*

Albert Einstein

Setting the Scene for International Debate

*left:
Prof. James
D. Bindenagel,
University of Bonn*

*right:
Dr. Mark Speich,
State of North
Rhine-Westphalia*

From September 30 to October 2, 2019, the *Center for Advanced Security, Strategic and Integration Studies* (CASSIS) and the *American Institute for Contemporary German Studies* (AICGS) hosted the 4th International Security Forum Bonn (ISFB). For the fourth consecutive year, the Forum convened more than 170 experts, researchers and policy makers from Europe, the United States, Russia, and China to debate some of the most pressing issues in contemporary international foreign and security policy.

Leading up the conference, **U.S. Consul General Fiona Evans'** keynote speech at the Dinner Talk on the eve of September 30th already shed a light on the numerous destabilizing trends and growing discord even among traditional allies, which are currently hampering efforts to address joint global challenges.

As **Prof. James D. Bindenagel**, former Director of CISG and Senior Professor at the newly established Center for Advanced Security, Strategic and Integration Studies (CASSIS), emphasized in his opening remarks during the main conference, the deep rifts in the current global order have only become more pronounced over the last few years. The international climate is increasingly marked by antagonistic thinking, the rise of a new nationalism and authoritarianism, and heightened political tensions that are expanding into uncharted territory such as space and the cyber realm. Europe for its part is caught between its two most important trading partners, the United States and China, both of which approach the world as an arena of competing interests and power struggle. The key question Western societies are faced with today, Prof. Bindenagel observed, may be an existential one: Does the world still need the West and other open democratic states to uphold a global order shaped by liberal values?

During his welcoming remarks, **Prof. Dr. Volker Kronenberg,** Dean of the Faculty of Arts of the University of Bonn, pointed out that the German federal government and the North Rhine-Westphalian state government have taken note of these fundamental changes in national and global politics as well. A key component of the government's strategy in addressing the new challenges of our time is to promote research on international relations, global interdependencies, and foreign policy in Germany and Europe. The University of Bonn has already made some strides in further contributing to this over the last years: Its establishment of CISG, the recent expansion into CASSIS and their most visible example of success, the ISFB, bear witness to that.

As the unraveling of the current international order urgently calls for discussions about where liberal democracies are headed, **Jeffrey Rathke**, President of the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University, pointed to the importance of open channels and cooperation – even, or especially, in times of tension between the transatlantic partners. In view of increasing friction on the international stage, he noted that efforts to bring people together, share views and disagree constructively are urgently needed.

In a similar vein, **Dr. Mark Speich,** Secretary of State for Federal, European and International Affairs for the State of North Rhine-Westphalia, highlighted during his address to the Forum that the tectonic shifts in international politics make mutual understanding, nuanced discussions and knowledgeable insights into the complex challenges of the twenty-first century more important than ever. As the cornerstones of the current global system are revealing themselves to be less durable than expected, it is crucial to properly understand the complex changes in the global environment in order to navigate these unchartered waters, lending formats such as the ISFB a particular relevance.

left:
Fiona Evans,
U.S. Consulate General
Düsseldorf

right:
Jeffrey Rathke, AICGS

List of Participants

Jonas Abs
Chairman of the DGAPforum Bonn, German Council on Foreign Relations (DGAP)

Philip Ackermann
Project Manager International Security Forum Bonn, Research Fellow, Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn

Victoria Appelbe
Director, Office of Economic Development, City of Bonn

Sophie Arts
Program Coordinator, Security and Defense Policy, German Marshall Fund of the United States (GMFUS)

Dr. Benjamin Becker
Managing Director, Amerika Haus e.V. NRW

Simone Becker
Research Fellow, Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn

Tjorven Bellmann
Acting Security Policy Director, Federal Foreign Office

Dr. Vladislav Belov
Deputy Director of the Institute of Europe and Chief of the Center for German Studies, Russian Academy of Sciences

Ambassador (ret.) Prof. James D. Bindenagel
Senior Professor, Former Head of the Center for International Security and Governance, Founding Henry-Kissinger-Professor, University of Bonn

Dr. Antoine Bondaz
Head of Program and Research Fellow, Fondation pour la recherche stratégique , Associate Professor, Sciences Po

Ann-Kathrin Büüsker
Journalist, Deutschlandfunk

Dr. habil. Landry Charrier
Attaché for Higher Education at French Embassy (NRW, Rhineland-Palatinate, Hesse and Saarland) and Director Institut français Bonn

Dr. Dean Cheng
Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy, Heritage Foundation

Dimitria Clayton
Policy Officer, State Chancellery North Rhine-Westphalia

Arash Duero
Senior Research Fellow, European Centre for Energy and Resource Security, King's College London

Fiona Evans
U.S. Consul General, U.S. Consulate General Düsseldorf

Dr. Marian Feist
Senior Research Associate, Institute for Environment and Human Security, United Nations University

Dr. Enrico Fels
Managing Director of the Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn

Dr. Peter Fischer-Bollin
Deputy Head, Department European and International Cooperation, Konrad-Adenauer-Foundation (KAS)

Dr. Ulrike Franke
Policy Fellow, European Council on Foreign Relations (ECFR)

Benjamin Fricke
Desk Officer for Security Affairs, Konrad-Adenauer-Foundation (KAS)

BrigGen Gerald Funke
Head of Division, Strategic Defence Planning & Concepts, Federal Ministry of Defence

Lea Gernemann
Policy Advisor, Population Dynamics, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Dr. Oliver Gnad
Co-Founder and Managing Director, Bureau fuer Zeitgeschehen

Prof. Dr. Malte Göttsche
Junior Professor for Experimental Physics, Aachen Institute for Advanced Study in Computational Engineering, RWTH Aachen

Dr. Shivam Gupta
Researcher, Bonn Alliance for Sustainability Research/ Innovation Campus Bonn (ICB)

Dr. Mischa Hansel
Research and Programme Coordinator, Development and Peace Foundation

Dr. Michael Hartlieb
Fellow for Theology and Philosophy, Thomas-Morus-Academy Bensberg

Prof. Dr. Andreas Heinemann-Grüder
Senior Researcher, Bonn International Center for Conversion (BICC)

Dr. Niklas Helwig
Senior Research Fellow, Finnish Institute of International Affairs in Helsinki

Prof. Dr. Dr. h.c Matthias Herdegen
Director, Institute for Public International Law and Institute for Public Law, University of Bonn

Dr. Sven Herpig
Head of International Cyber Security Policy, Stiftung Neue Verantwortung

GenLt (ret.) Kurt Herrmann
President of the Clausewitz Society

Prof. Dr. Wolfram Hilz
Professor for Political Science and Acting Director of the Center for Advanced Security, Strategic and Integration Studies, University of Bonn

Goos Hofstee
Research Fellow, Clingendael Institute

Austin Hudgens
Administrative Assistant at Clearlake Capital Group LLC

Dr. Jackson Janes
Senior Fellow at the German Marshall Fund, President Emeritus, American Institute for Contemporary German Studies (AICGS), Johns Hopkins University, Washington D.C.

Dr. Karsten Jung
Head of the Strategy Department, Ministry of Finance of North Rhine-Westphalia

Dr. Katharina Kaesling
Research Coordinator, Käte Hamburger Center for Advanced Study „Law as Culture", University of Bonn

Prof. Dr. Dr. h.c. Karl Kaiser
Senior Fellow, Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Adj. Professor of Public Policy emeritus, Harvard Kennedy School

Katharina Kiefel
Program Manager, Amerika Haus e.V. NRW

Dr. Alexander Klimburg
Director of the Cyber Policy and Resilience Program, The Hague Centre for Strategic Studies

Dr. Christian Koecke
Coordinator for Policy Issues and Transatlantic Relations, Political Education Forum NRW, Konrad-Adenauer-Foundation (KAS)

Wolfgang Kopf, LL.M.
Senior Vice President for Group Public and Regulatory Affairs at Deutsche Telekom AG

Prof. Dr. Volker Kronenberg
Dean of the Faculty of Arts, University of Bonn

Alexander Graf Lambsdorff
Deputy Chairman of the Group of Free Democrats, German Bundestag

Arthur Laudrain
Global Scholar for Peace, Conflict Prevention and Resolution, Rotary Foundation

David Llorens Fernández
Vice President of the University of Murcia Chapter, European Horizons

Goodarz Mahbobi
CEO, axxessio GmbH

Col i.G. Soenke Marahrens
Program Director, German Institute for Defence and Strategic Studies (GIDS)

Karina Marzano
Associate Fellow at the Institute for Advanced Sustainability
Studies (IASS), Potsdam

Prof. Dr. Carlo Masala
Professor for International Politics, Bundeswehr
University Munich

Dr. Maximilian Mayer
Assistant Professor in International Studies, School of
International Studies, University of Nottingham Ningbo China

Dr. Nicolas Mazzucchi
Research Fellow, Fondation pour la recherche stratégique

Prof. Dr. Holger Mey
Vice President, Head of Advanced Concepts, Airbus Defence
and Space

Dr. Ute Meyer
Public Affairs and Government Relations Specialist,
U.S. Consulate General Düsseldorf

Hanna Müller
Head of the Division "Political Systems, Militant Democracy",
Federal Ministry of the Interior, Building and Community

Carisa Nietsche
Research Assistant, Transatlantic Security,
Center for a New American Security (CNAS)

Dr. Hendrik Ohnesorge
Research Fellow and Managing Assistant at the Center for
Global Studies (CGS), University of Bonn

Prof. Dr. Alice Pannier
Assistant Professor, Paul H. Nitze School of Advanced
International Studies (SAIS), Johns Hopkins University,
Washington D.C.

Alexandra Paulus
Doctoral Student, TU Chemnitz

Dr. Jana Puglierin
Head of the Alfred von Oppenheim Center for European
Policy Studies, German Council on Foreign Relations (DGAP)

Jeffrey Rathke
President of the American Institute for Contemporary German
Studies (AICGS), Johns Hopkins University, Washington D.C.

Dr. Benjamin Rhode
Research Fellow for Transatlantic Affairs, Editor Strategic
Comments, International Institute for Strategic Studies

Prof. Dr. Jakob Rhyner
Professor for Global Change and Systematic Risk,
Academic Director for the Innovation Campus Bonn,
University of Bonn

Frank Rose
Senior Fellow for Security and Strategy, Foreign Policy
program, Brookings Institution, Former Assistant Secretary
of State for arms control, verification, and compliance

Dr. Norbert Röttgen
Chairman of the German Bundestag Committee on
Foreign Affairs

Peter Rough
Fellow, Hudson Institute, Washington D.C.

Prof. Dr. Jürgen Rüttgers
Federal Minister of Education, Science, Research and
Technology (ret.), Prime Minister of North Rhine-Westphalia
(ret.), Special Adviser to the EU Commission,
Honorary Professor of the University of Bonn, Institute of
Political Science and Sociology, Honorary Fellow of the
Interdisciplinary Center (IDC) Herzliya, Israel

Kaan Sahin
Research Fellow, Technology and Foreign Policy, German
Council on Foreign Relations (DGAP)

Lewis Sanders
Multimedia Journalist, Deutsche Welle

Dr. Dimitri Scheftelowitsch
Software Engineer, ESR Labs, Munich

Prof. Dr. Conrad Schetter
Professor for Peace and Conflict Studies, and Director for
Research, Bonn International Center for Conversion (BICC)

Christian Schmickler
Cluster Manager, Cyber Security Cluster Bonn e.V.

Julian Schmidt
Market Analyst in Strategic Marketing, Airbus

Arne Schönbohm
President of the German Federal Office for Information
Security (BSI)

GenMaj Jürgen Setzer
Vice Chief of the Cyber- and Information Domain Service and
Chief Information Security Officer of the Bundeswehr

Prof. Dr. Yi Shen
Associate Professor, School for International Relations and
Public Affairs, Fudan University

Ludger Siemes
Head of European and International Affairs, State
Chancellery of North Rhine-Westphalia

Prof. Dr. Matthew Smith
Professor at the Institute of Computer Science,
University of Bonn

Dr. Mark Speich
State Secretary for Federal, European and International
Affairs of the State of North Rhine-Westphalia

Frank Sportolari
President of UPS Germany

Ashok Sridharan
Lord Mayor, City of Bonn

Ambassador (ret.) Dr. Volker Stanzel
Senior Distinguished Fellow, German Institute for
International and Security Affairs (SWP),
Former German Ambassador to China and Japan

Gertrud Sterzl
Journalist, West German Broadcasting (WDR)

Marcel Stolz
DPhil Candidate in Cyber Security, University of Oxford

Jan Ternberger
Master student, HEC Paris and FU Berlin

Tara Varma
Head of the Paris Office & Policy Fellow, European Council on
Foreign Relations (ECFR)

Ignacio Villalonga
Strategic Market Forecast, Airbus

Michelle Combs Watson
President and CEO of Cyber Intelligent Partners (CIP)

Thomas Wiegold
Editor „Augen Geradeaus!"

Nils Wörmer
Head of Department Foreign, Security and European Affairs,
Konrad-Adenauer-Foundation (KAS)

Dr. Anja von Wulffen
Desk Officer, Division Critical Infrastructure Protection (CIP)
Strategy, Cyber Security CIP, German Federal Office of Civil
Protection and Disaster Assistance (BBK)

Yixiang Xu
New Research Initiative Fellow, American Institute for
Contemporary German Studies (AICGS), Johns Hopkins
University, Washington D.C.

Lauren Zabierek
Executive Director, Cyber Security Project, Belfer Center for
Science and International Affairs, Harvard Kennedy School

Dr. Martin Zapfe
Assistant Branch Chief, Multinational Capability Development,
Federal Ministry of Defence

Dr. Zhexin Zhang
Research Fellow, SIIS Deputy Editor, China Quarterly
of International Strategic Studies

as of September 27, 2019

Executive Summary

At the dawn of the 2020s, is has become clear that many of the expectations that accompanied the turn of the millennium have not been fulfilled. After the fall of the Berlin Wall, many policy makers and analysts hoped that liberal democracy would spread throughout the world in a linear manner and usher in a new, more peaceful era of international relations. Three decades later, the "end of history", as coined by political scientist Francis Fukuyama, has not yet materialized. The global political climate today is marked by a new competitive edge in international politics, the rise of systemic challenges to liberal democracy, and heightened political tensions between old rivals just as much as between longstanding allies. These developments are accompanied by a growing number of new cross-border security challenges in international politics and security that seem increasingly difficult to tackle in an atmosphere of distrust and renewed zero-sum-thinking.

The 2019 International Security Forum in Bonn aimed to examine these trends from two specific perspectives: The first session was concerned with the West's prospects during a time when many of the premises of European foreign policy are contested and Western global influence is declining. What oversights or mistakes caused liberalism's current crisis? In what ways may political leaders on both sides of the Atlantic be able to address internal and external challenges? Will the West in its previous form unravel, reform itself, or enter a new path entirely to adapt to a changing world? Second, the 2019 Forum aimed to provide an outlook toward the key emerging state that many

international observers believe to be a particular test for what is commonly referred to as the international liberal order: the People's Republic of China's global ascent. What drives Chinese foreign policy? What could be China's long-term goals with regard to reshaping the international system to better reflect its own interests? And how should global leaders react to shifting power relations?

Prof. Dr. Volker
Kronenberg,
University of Bonn

The 2019 ISFB saw a large number of heterogeneous views and vigorous debates, especially regarding the question of how European states should aim to realign themselves as they are is unexpectedly finding themselves in a world of renewed power politics and transactional relations. In Europe and beyond, the continent is increasingly seen as the playground where new power competition plays out, putting especially the EU's foreign policy model under pressure. Europe, it seems to many observers, is (again) turning into an object of global power play rather a capable subject able to shape its own future.

The Forum revealed a broad consensus that Europe does not appear well-prepared to cope with the unprecedented challenges for its foreign policy that has been founded on a global framework largely sustained by the United States. The continent remains preoccupied with internal divisions and crises, but discussions underlined what one participant called the "primacy of foreign policy": Addressing urgent foreign policy issues cannot wait until internal issues are resolved. Between diverging national priorities and a currently limited ability to act on a global scale, the EU in particular needs to define a path forward. The Forum highlighted that in terms of foreign policy, Europe is confronted with the challenge to balance various existential objectives: addressing the serious threats to its security and stability while maintaining its overarching goal of exerting a civilizing influence on global affairs and safeguarding its normative core that it established after experiencing the devastating consequences of great power politics on its own soil.

With view to China, the 2019 ISFB revolved around the observation that the world is witnessing what some call rise and others call return of the Middle Kingdom. While Beijing asserts that China's peaceful recovery of its historic place within the global community comes with no threat to other states, many neighboring countries are observing China's increasingly assertive policies with suspicion. Much of the Asia-Pacific, but also Europe and North America, is reacting negatively to the recent revival of Chinese nationalism and Beijing's ambiguity regarding its commitment to multilateralism and international law, as well as its lack of reciprocity in trade – which, notably, Beijing is starting to realize.

The session emphasized that the Middle Kingdom's reemergence as a global power opens up the potential for both competition and cooperation vis-à-vis other actors. A continuous dialogue may help to demystify common misconceptions, improve mutual understanding, and deescalate tensions. At the same time, discussions highlighted a growing number of conflicts in areas such as trade, technology and conflicting attitudes towards key political concepts, such as the national sovereignty or the rule of law in contrast to the "rule by law". Combined, these conflicts and differing perspectives are likely to lead to a new set of challenges for international politics that will need to be addressed urgently.

The Special Focus Day, a new feature within the Forum's established structure, was dedicated to a specific policy area: the new and emerging challenges in the realm of cybersecurity and artificial intelligence (AI). With this new format, the 2019 Special Focus Day, conducted under the auspices of North Rhine-Westphalia's former Minister President Prof. Dr. Jürgen Rüttgers, aimed to shed a light on how the enormous technological strides in these areas are changing international relations.

The conference highlighted that the cyber sphere is becoming a part of a global trend that revolves around escalating competition, distrust and a lack of norms for acceptable international behavior. Cyber is a moving frontier that confronts policy makers and governments with numerous new challenges, including issues such as blurring lines between war and peace, enormous difficulties in regulating and monitoring cyber activities, and a growing power imbalance vis-à-vis the private sector. Debates also pointed to a dangerous tendency to divorce the digital from the physical world, and to subsequently severely underestimate the consequences that may result from a failure to prevent political conflicts from expanding into the cyberspace. Though the Forum revealed much skepticism among experts about how well global governance is currently equipped to deal with the unique challenges of cybersecurity, the Special Focus Day showed the urgent need to create internationally accepted standards in the cyberspace.

Despite a large variety of perspectives, the 2019 Forum closed with a clear bottom line. We are currently entering a new phase of international relations that is marked by the upheaval of seemingly entrenched political structures, serious developments in the fields of cybersecurity and modern warfare, and a dangerous revival of antagonistic power politics and transactional relations. These developments are accompanied by the emergence of new actors that capitalize on technological advancements without adhering to state-centered multilateral agreements, and multi-dimensional, long-term challenges such as climate change that extend well beyond the national realm. As a result, states are confronted with a whole host of new issues that have the potential to critically disrupt entire societies, while they are at the same time left with decreasing room to achieve their international goals unilaterally.

While the current shift in global politics does not inevitably have to lead to a Third World War, as many international observers are increasingly warning, heightened tensions and renewed power politics certainly increase the chances of violent escalation, even if only accidental or as the result of political miscalculation.

Dr. Oliver Gnad,
Bureau für Zeitgeschehen

The 2019 Forum also revealed that many of the structures designed to help stabilize the global environment during the second half of the twentieth century are becoming increasingly ineffective or are entirely missing today. While many participants sharply criticized calls to resurrect Cold War structures in a world that looks wildly different from that of the twentieth century, the global community so far has proven largely incapable of finding comprehensive responses to today's challenges.

In his concluding remarks, Prof. Dr. Dr. h.c. Karl Kaiser noted that approaching the growing number of threats to international security and peace will require global leaders to start thinking in global terms and abandon zero sum thinking. The 2019 ISFB highlighted that the need to organize collective action for global common goods and to address shared threats are bound to remain a key element of world politics. In particular, participants pointed to the urgent need to establish more effective frameworks for cooperation to manage the use of the sea, space and the cyber

realm as well as the effects of climate change, and to mitigate the risks of escalating tensions between states. As power is shifting horizontally as well as vertically and states' abilities to reach their global goals on their own is decreasing, it appears likely that the international order will undergo some fundamental transformations, and that current global frameworks will have to be adapted to better reflect today's changing realities.

For open democratic societies, this may mean that likeminded countries may have to come together to project a common vision of the world, supported by an underlying agreement on fundamental principles and values, if they want their values and ideas to be represented in this transforming order. After the West has increasingly turned to nostalgia, defensiveness, or at times even to a self-defeating abandonment of liberal ideas, the key challenge for liberal democracies may be to formulate a more sustainable positive vision for their future.

Session I:
The West's Perspectives in a Changing Global Order

Key points

- The crisis of what is commonly referred to as the international liberal order has sparked a fierce debate about the merits and perspectives of liberalism. In the West, the turn-of-the-millennium optimism about liberalism's superiority has largely given way to defensiveness, nostalgia, or a tendency to question liberal values.

- Against the backdrop of a surge of antiliberal backlash and renewed global competition, Europe is finding itself in an unexpected global position. Mounting challenges such as decreasing commitment to multilateral cooperation, intensifying confrontations with Russia, and growing instability in the MENA region are putting especially the EU's foreign model under pressure.

- Europe's internal divisions and crises hamper a coherent foreign policy, which may become a threat to European stability. The continent is faced with the challenge to balance its values and the overarching goal of exerting a civilizing influence on international relations with the need to become more resilient against possible threats to its way of life.

- If open democratic states want their political values and principles to be reflected in a transforming world order, this may require like-minded countries to focus on addressing their internal deficits, strengthening their social, political and infrastructural resilience, bolstering alliances, identifying common goals and creating leverage to jointly realize a shared vision of the world.

- While contested from many sides, liberal ideas may help provide solutions to today's challenges if adapted appropriately. The key challenge may be for liberal democracies to develop a positive vision for the future underpinned by a shared understanding of fundamental political values.

Dr. Norbert Röttgen, German Bundestag, Frank Rose, Brookings Institution, Lauren Zabierek, Belfer Center at Harvard's Kennedy School

*Dr. Jana Puglierin,
German Council on
Foreign Relations (DGAP)*

Over recent years, the end of liberal hegemony and the unraveling of the frequently cited global liberal order have been on everyone's lips. As the eulogies are pouring in, liberalism as an organizing principle of international relations as well as state organization is with equal vigor defended by some and attacked by others. While its global dominance is declining, liberalism seems to be turning into an even more fiercely disputed concept.

Part of these contentions are due to the fact that the liberal order, frequently accompanied by vague references to the rule of law, is somewhat of an ambiguous buzzword that is underpinned by a complex and often contradictory political reality. Furthermore, the fact that many liberal democracies' foreign policy has frequently been inconsistent with its own values has not only raised questions about its normative legitimacy, but is also complicating debates about the lessons from liberalism's current crisis. The 2019 ISFB mirrored many of the diverging viewpoints and conclusions that its current crisis has provoked among analysts and policy makers.

As one participant laid out, U.S. foreign policy in the late 1990s and 2000s was largely informed by what was called Convergence Theory and aimed to integrate emerging and non-Western states – most notably Russia and China – into a global system that sought global stability through the spread of liberal democracy under U.S. leadership. According to various voices at the Forum, that approach had a critical flaw: Western leaders massively underestimated the degree to which other states considered this Western-centric system a threat to their interests, identities, or regime legitimacy. For instance, one speaker argued that U.S. leaders failed to recognize longstanding sentiments among Russian officials that the INF Treaty and other legal frameworks were marked by an imbalance in favor of the U.S. and forced upon Russia. As a result, the collapse of the INF in 2019 may be seen as a prime example of a much larger global trend that sees non-liberal states pushing back.

Aside from revisionist powers who challenge a system dominated by the U.S. throughout much of the last century, liberalism's global vision is contested from many other sides as well – most notably its main stakeholder. At the 2019 ISFB, various experts from the U.S. reported that Washington is increasingly dominated by the view that multilateral institutions may help provide global stability, but overall only set up the parameters for global power politics: For U.S. president Donald Trump and like-minded politicians in the U.S. and beyond, politics are increasingly driven by a competitive mindset that may consider multilateralism as a tool, but not as an inherent priority. On the contrary, the current U.S. government does not consider most pressing political matters to be questions of legality.

Many participants supported the prediction that the competitive urge in international politics, paired with an increasingly narrow understanding of national interests, are likely to remain strong as global power continues to shift. Various U.S. experts also agreed that interventionist tendencies in U.S. foreign policy are a thing of the past and may have seen their last gasp in Libya when the 2005 UN principle Responsibility to Protect (R2P) was still a relevant factor.

Europe in a Changing Global Environment

With view to Europe, participants reached a broad consensus that today's large global trends constitute unprecedented challenges for European foreign policy. For the past seven decades, much of Western Europe and the European Union developed its foreign policy identity based on the idea of a civilian power that was situated within a global framework largely sustained by the U.S. Nowadays, post-Cold War Europe is increasingly seen as the playground where great power competition plays out, putting especially the EU in an entirely unexpected position and the EU's foreign policy model under pressure. For EU member states, the key question addressed during the Forum was how to persist in a world of increasingly transactional relations and zero-sum thinking without renouncing the standards and norms that they established after first-handedly experiencing the devastating lessons of great power politics.

The Forum revealed a broad range of views as to what conclusions EU member states should draw from current developments and how to react to the array of challenges that the rise of antiliberal forces may entail. Notably, the discussions reflected growing support for a firmer approach to foreign policy that focuses on identifying and protecting EU interests and values, warding off authoritarian assertions and disruptions,

and mitigating the effects of the U.S. retreating from the transatlantic partnership. One speaker made the case for a double strategy of "deterrence and dialogue" that consists of firmly defending Western values and interests against outside assertions combined with robust dialogue based on an updated system of norms for international behavior shared by all actors. Examples like the recent conflict in the Strait of Hormuz indicate, another participant argued, that Europe will have to learn to defend its own interests because no one else will: As the confrontation with Moscow is hardening, the Trump has declared the EU a "foe" to the U.S., and Europe's neighboring regions are marked by instability, the EU's current foreign policy approach may put Europe in a position of severe vulnerability.

On the other hand, various participants argued that liberal democracies need to double down on their values in foreign policy in order to maintain integrity and credibility as a counterexample to authoritarian, nationalist and illiberal attitudes and renewed power politics. Arguing that liberalism has been a forward-thinking force for good in the world, various participants called for Europe to maintain its civilizing influence on international affairs, focus on enhancing cooperation to promote a positive vision for a peaceful global environment, and steer away from a return to the power politics of the past.

Frank A. Rose,
Brookings Institution

Dr. Alice Pannier,
Johns Hopkins University
and Peter Rough,
Hudson Institute

The EU's Dilemma

Europe's dilemma of trying to find a balance between its normative goals and its more imminent challenges in foreign and security policy, which may soon turn into a vital threat to European stability, led one speaker to come up with the most memorable metaphor of the conference: Calling for the EU to become a "Brachiosaurus" of international affairs , she argued for the EU "to remain a vegetarian in a world of meat eaters, but one that is so massive and powerful that it is impossible to eat." Under the motto United we stand, divided we fall, she made the case for a "smart adaption": strengthening the EU in the area where it is strong, using the EU's joint weight to actively shape the international normative and regulative environment, and adapting an anticyclical stance to serve as a reference point for the "carnivores out there," all while acknowledging the changing global realities and acquiring the ability to take charge of its own security.

However, the experience of recent years shows that EU member states have had difficulties to overcome national differences and act as a unified global player in almost all areas of foreign policy. Debates at the Forum also mirrored some of the diverging viewpoints on the goals and means of EU foreign policy, such as during a heated discussion about the merits of coalitions of the willing, which were considered a threat to European cohesion by some and a pragmatic option to dealing with Brussels' foreign policy gridlock by others. It also became clear throughout the discussions that, even if member states manage to overcome their inability to agree on coherent EU positions, they still lack the practical means to pursue a truly sovereign foreign policy.

Tjorven Bellmann, Federal Foreign Office and Dr. Jackson Janes, AICGS

Resilience, Alliances, and International Influence

Many of the suggestions presented during the 2019 ISFB centered around three core pillars: Alliances, resilience, and the shaping of the international environment. The West's ability to maintain close networks that are bound together by shared values and solidarity, not just out of necessity, were considered to be the key asymmetrical advantage vis-à-vis Beijing and Moscow. Beyond strengthening the cohesion of existing alliances, it was also argued that liberal democracies should further focus on "finding and fostering pro-liberal alliances": Liberal principles may have been the product of the enlightenment, one participant argued, but much of its appeal extends well beyond the Western Hemisphere.

Second, many experts present at the Forum pointed to the critical importance of resilience in the face of external and internal disruptions and assertions. Recommendations for how to boost domestic resilience included addressing the political and economic roots of grievances in national electorates and the resulting surge of populist and illiberal forces; protecting the integrity of electoral processes and democratic infrastructure; addressing internal democracy deficits that undermine their normative credibility; and protecting the resiliency of critical infrastructure against attacks.

Third, many arguments revolved around options and perspectives for Europe and other like-minded states to use their joint weight to actively shape the international environment and compete for norms and influence. This may include collectively pushing back against authoritarian efforts to downgrade human rights and other core principles; more realistically assessing areas where emerging powers exert influence and counterbalancing those efforts with own initiatives; helping to adapt international institutions to the realities of the twenty-first century; and collaborating in shaping the rules and norms on emerging technologies as well as the use of outer space.

Liberalism from a Twenty-First Century Perspective

The 2019 ISFB illustrated that, after the euphoria of the 1990s that saw Western ideas as the crowning of history, contemporary debates in Western intellectual and political circles are often marked by the opposite tendency to consider liberalism with a sense of defensiveness, nostalgia, or even the tendency to question liberal ideas altogether. Overall, the discussions throughout the 2019 ISFB largely clustered around two of the largest intellectual camps in these debates. Echoing thinkers such as John Mearsheimer, the conclusion for some was that liberalism's current crisis indicate

that efforts to transcend realist thinking and ensure lasting global stability through civilization and liberalization have failed. According to these voices, cooperation may still be possible in some areas, but a return to the status of the 1990s and early 2000s is unlikely.

On the other hand, debates also highlighted that today's volatile global environment may in fact lend many of liberalism's key premises renewed relevance. It was precisely liberalism's acute attentiveness to the possibilities of large-scale catastrophe in a highly interconnected, technologically advanced and environmentally vulnerable world that has prompted the establishment of an open, rules-based multilateral order as a pragmatic approach to de-escalating tensions and securing global common goods. Many participants' conclusions during the Forum were reminiscent of thinkers such as Daniel Deudney and John Ikenberry, who argued in 2017 that, even though it no longer seems inevitable that the global order will end up liberal in the long-term, liberal ideas could contribute to making it a more decent one. Debates revealed that, if adapted appropriately to a more complex global reality, they may help provide answers to global challenges – providing that liberal democracies formulate a positive and more sustainable vision for the future that addresses the flaws and inconsistencies of the last decades. Various participants also emphasized that

open democratic systems improved living conditions for billions of people worldwide and significantly contributed to global stability in the twentieth century. As Turkish political scientist Selim Sazak pointed out in 2018, establishing an open democracy "remains a political goal for countless political actors around the world independently fighting to achieve it at home."

One speaker argued during the Forum that the so-called liberal order has to some degree always been a common narrative among like-minded states that may even have been just as powerful than the practical realities behind it. Currently, changing priorities and the loss of a common language within the liberal community threaten to weaken the fabric that has made the alliance strong. Removing the coat of this common narrative is now revealing the underlying divergences and reducing the chances for automatic alliances. If the adhesive glue falls away in favor of a more pragmatic approach based on bilateralism, individual initiatives, and ad hoc coalitions, one participant raised the question whether the whole of these initiatives will be more than the sum of its parts – and whether that will be enough to serve as a countermodel to illiberal and authoritarian forces that aim to reshape the international environment according to their preferences.

Hanna Müller, German Federal Ministry of the Interior, Building and Community

The Bonn Power Shift Monitor

In his keynote speech that rang in the second session of the 2019 ISFB, Dr. Hendrik Ohnesorge from the University of Bonn's Center for Global Studies offered a glimpse into global power shifts from the perspective of empirical research: Discussing the phenomenon of shifting power as a constant in international affairs and offering a glimpse into his Center's research, he presented the latest issue of the Bonn Power Shift Monitor (BPSM) in order to provide an empirical footing for the 2019 ISFB debates.

Dr. Hendrik W. Ohnesorge, University of Bonn

Greatly Exaggerated: China's Rise and America's Decline in the Light of the Bonn Power Shift Monitor

by Hendrik W. Ohnesorge & Christiane Heidbrink

Being confronted with reports of his own demise, Mark Twain is said to have quipped in 1897, "The reports of my death are greatly exaggerated."[1] In view of the latest findings of the Bonn Power Shift Monitor (BPSM),[2] much the same can be said concerning the ongoing debate on the rise of China and a concurrent decline of the United States of America.

China has undoubtedly presented an extraordinary rise over the past decades. It is the biggest gainer in global power shares according to the BPSM, whereas the United States shows the reverse trend. At first glance, it seems as if the USA is inevitably doomed to decline because it lost considerable amounts of power shares in the past. Recent figures, however, suggest that this trend might soon come to an end as the

---

1   For Twain's actual quote and its evolution, see Ralph Keyes, The Quote Verifier: *Who Said What, Where, and When* (New York: St. Martin's Griffin, 2006), p. 42.
2   For the full report and further analyses, see Center for Global Studies, "Bonn Power Shift Monitor," online at: https://www.cgs-bonn.de/de/bonn-power-shift-monitor/.
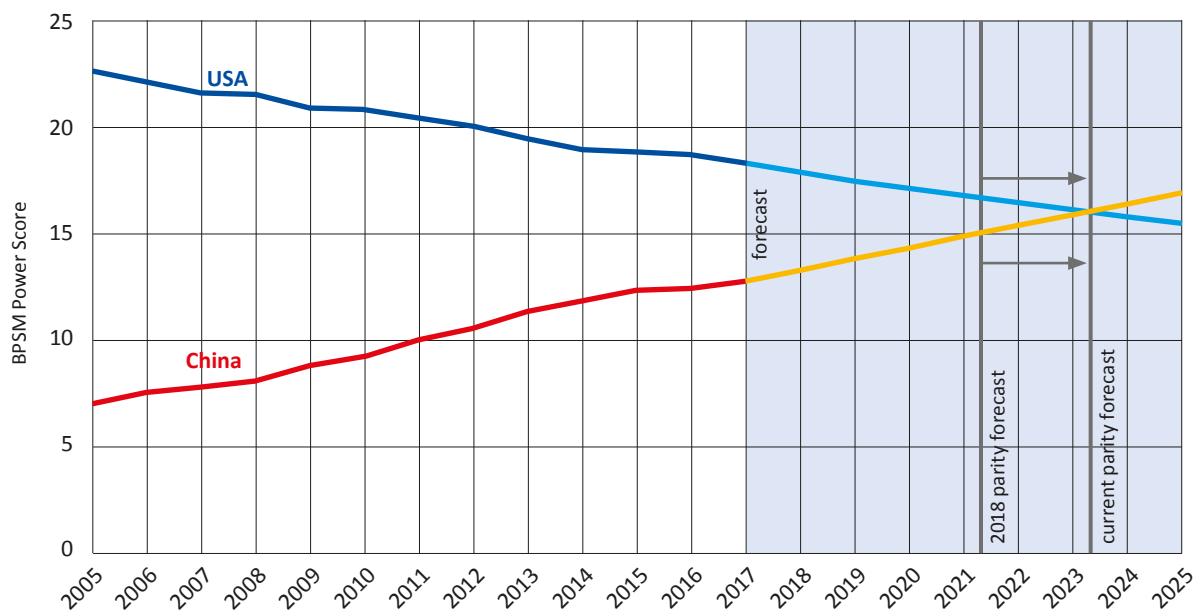
Power Shift Forecast: USA and China

Chart: Center for Global Studies (CGS) – Heidbrink. Source: Bonn Power Shift Monitor (BPSM) 2020

BPSM notes a significant slow-down of both the rising China and the declining USA. The 2018 forecast thus predicted a power parity between the two states in 2021. Due to China's weakened growth rates and the United States' recent upturn, this "doomsday" is now predicted for mid-2023 – and might even be further delayed.

Decline and rise are yet inextricably linked if one conducts a relative power measure. This measure does, however, not tell anything about the absolute developments within the countries of interest. In absolute numbers, the United States has not lost power. Quite the contrary, the BPSM records a positive growth average. Indeed, the rate is much smaller than that of developing countries like China or India – but this holds true for all the industrial, highly-developed states. This trajectory is similar to what we know from every role-playing game. It is much easier to level-up in the beginning of a game, while it requires much more effort on a higher level. Therefore, both types of measurement – relative and absolute – do neither indicate an incessant decline of the USA nor an irresistible rise of China.

In the light of these findings, several observations can be made: First, the United States continues to be the most powerful country in the world – in fact, with a considerable margin and ranking No. 1 in five out of the eight categories considered in the BPSM. Second, while certainly verifiable through the BPSM in the long run, the trends of both China's rise and America's decline have considerably slowed down in the most recent period under review (2015-17). Third, and as a consequence, all parties would do well to take the edge off the current discourse on the alleged changing of the guard on the international scene, a process which in the past has frequently led to conflicts between the established and the rising power. After all, given the plethora of challenges facing international relations today, a more cooperative relationship between Washington and Beijing would indeed be welcome.

Session II:
China on the World Stage

Key points

■ Rather than an emerging power, China is better characterized as a returning power whose foreign policy is informed by the goal to recover its historic global position. It relies on a comprehensive understanding of power and security that is based on a strong political and territorial union and includes scientific and technological prowess, cultural security, and political recognition in international institutions.

■ While Beijing claims that its goal to peacefully ascend within the global order does not pose a threat to other countries, many neighboring countries as well as the U.S. and Europe are observing China's increasingly assertive policies, its rapidly growing power resources and power projections, and its ambivalence towards its legal obligations with caution.

■ Conflicting interests in areas such as trade and technology as well as contrasting approaches to key political concepts such as national sovereignty and the rule of law are likely to lead to a new set of challenges for international politics.

■ As China competes for global influence with numerous other players, organizing collective action remains imperative in a highly interconnected world. Vertical and horizontal shifts of power make changes to the international system highly likely and will require the international community to develop a new framework that addresses more complex global realities with rules for international behavior shared by all actors.

■ The key question for international security in the upcoming century may be how well the great powers – particularly China and the United States – will be able to work together on these challenges.

*Ambassador (ret.)
Dr. Volker Stanzel,
German Institute for
International and
Security Affairs (SWP)*

The U.S. defense strategy, like many American and European observers, classifies China as a "revisionist power". Debates during the 2019 ISFB revealed that in order to gain a more differentiated picture of global developments, China is better characterized as a returning power with grievances. The rhetoric of Chinese officials and media outlets confirm that China does not consider itself a rising power: As one speaker outlined, the Chinese Dream is firmly rooted in the goal of reviving the Chinese people and reinstating its historic greatness after the Century of Humiliation, a term that is used in China to describe a period of West European, American and Japanese interventionism and imperialism between 1839 and 1949. The experience of collective humiliation through the temporary loss of sovereign control over its own territory, borders, and national destiny plays a crucial role in how Beijing frames and aligns its foreign policy.

Against this backdrop, the 2019 ISFB revealed that one key component to understanding China's global goals may be the Chinese concept of deterrence. Better translated into English as "compellence," Beijing's understanding of deterrence implies a much more comprehensive concept: Beyond economic and military strength, it focuses on a broad understanding of power that is based on political and territorial union and includes elements of persuasion on all levels. For China, one expert explained, global power is also viewed as coherence, scientific and technological power, cultural security, and recognition similar to that of the United States, and political recognition and acknowledgement in global institutions and beyond. According to him, all measures of Chinese foreign policy are directed toward the goal of strengthening this comprehensive power.

Dr. Antoine Bondaz,
Fondation pour la
recherche stratégique

*Dr. Dean Cheng,
Heritage Foundation*

Chinese Power

Discussions at the 2019 ISFB in large parts revolved around China's growing global influence. As the Bonn Power Shift Monitor illustrated, China is rapidly becoming more powerful in terms of a range of different power indicators from economic strength to technological prowess. Already the most populous country in the world, it also appears to be gaining ground in a long-term race to becoming the strongest (see the "Bonn Power Shift Monitor" for more details).

Understanding the depth and possible implications of these developments requires a much more nuanced look, however. For instance, during the 2019 ISFB highlighted that the relationship between political clout, power resources, and the ability to influence global affairs is much more complex than these observations may suggest. As one participant pointed out, a nation's power surplus in relation to one or even all other actors does not automatically correspond with its ability to control the outcome of international conflicts. Classical considerations of power such as Max Weber's that focus on its practical use tend to overlook the passive impact of power. As Chinese power grows, one participant argued that this will also

increase gravitational forces that pull other countries further into China's orbit. This might soon put China in a similar position as that of the United States in the sense that large political, economic, or societal trends originating there have repercussions that can be felt throughout much of the rest of the world.

In the other hand, debates also highlighted that the frequent focus on quantifiable hard power resources neglects the impact of intangibles such as perceptions, feelings, and preferences and the ability to co-opt and persuade, or what Joseph Nye coined as "Soft Power" in 1990. In terms of Soft Power, one participant reported that the Chinese government estimates China to lag at least ten to twenty years behind the United States. The international community and particularly Asian neighbors observe Beijing's rise with a certain caution. This seems to be especially true when considering the period between 2010 and 2014, which Chinese foreign policy experts now refer to as a period of "strategic overreach." As Beijing increasingly openly projected a strong vision of Chinese leadership, evoking aspirations to grandeur in the Chinese public, the impression of revived Chinese nationalism has provoked negative feedback and a certain suspicion in other capitals.

As various participants pointed out, however, Beijing seems to have taken note of these developments. The Chinese government has since tried to tone down its overt foreign policy ambitions, notably working to establish better relations with neighboring countries since 2016. Still, in view of China's policies such as its complete lack of willingness to multilaterally solve the conflict in the South China Sea, discussions at the Forum reflected the impression among many observers that China seems to underestimate the impact its policies are having around the world, and the extent to which it is losing Soft Power.

China's Long-Term Goals

From a longer-term perspective, the Forum once more revealed that a glance at China's global ambitions and the implications this may have for the global order comes with many question marks. One participant argued that the global community should expect the exploitation of the current multilateral order based on the rule of law as promoted by the West, while China develops an alternative approach. The key factor that inhibits China from sustaining the current order in its

precise form in the long run, he argued, is that the concept of rule of law – the current order's backbone – doesn't exist in Chinese history, which has instead traditionally followed an approach that consists of the rule by law. It was also argued that the Russian-Chinese coalition has a single strategic goal, which is to balance U.S. power and mitigate Western democracies' influence as a shaping force of international relations. Then again, one Chinese insider argued that both Moscow and Beijing are "driven by a foreign policy vision that is shaped by power politics," which prohibits a truly equal and honest alliance. Thus, it also appears unlikely that Beijing will be able to form an overarching network similar to the transatlantic system.

Meanwhile, Beijing itself has been adamant in defending its claim to peacefully resume its seat in the middle of the global community without intending to constitute a threat to others, rejecting accusations of trying to achieve global dominance and upending order. According to one Chinese expert present at the Forum, Beijing aims to create "a norm of coordination among all powers in the region and mutual respect based on sovereignty". Certainly, the Chinese govern-

Dr. Antoine Bondaz, Foundation pour la recherche stratégique, Prof. Dr. Andreas Heinemann-Grüder, Bonn International Centre for Conversion, Dr. Jana Puglierin, German Council on Foreign Relations (DGAP)

ment remains restrained about voicing its global ambitions. As one participant pointed out, the Communist Party is unlikely to ever sound like President Trump. What's more, Chinese voices largely agree that Beijing is neither prepared nor willing to assume a global leadership role analogous to that of the United States. Especially in view of the substantial costs such a role implies, Beijing is more focused on consolidating its regional foothold and ensuring national unity and realizing its vision of territorial, political, and social unity.

Yet, China's policies such as its failure to practice full reciprocity on trade and its disregard of international law in the South China Sea are raising international doubts about the extent to which China is committed to legal frameworks, multilateralism, and international obligations. Furthermore, initiatives like the Asian Infrastructure Investment Bank as an alternative to the International Monetary Fund and the "Belt and Road" infrastructure development and investment initiative (BRI) illustrate Beijing's clear will to leave its mark on the global order. Many non-Chinese observers consider the BRI a major global project to deepen Chinese global influence that is designed to create dependencies. Since 2017, the BRI also includes a military bases in Djibouti, the first base outside Chinese territory. As a result, analysts are starting to see more and more parallels to more far-reaching global power projections similar to those of the United States in the early twentieth century.

Collective Action in a Changing World

The Forum highlighted that the international community should expect change without much doubt. Power is currently shifting from West to East; spreading towards a larger group of states as other economies such as India grow and U.S. relative power declines; and diffusing as the information revolution is empowering non-state actors such as corporations, terrorist organizations and even social movements, undermining the primacy of states in world politics. That also means that, as Joseph Nye argued in 2018, the terms "international liberal order" and "Pax Americana" may in some ways become outdated as descriptions of a world that looks exceedingly more complex than it was during the second half of the twentieth century.

So far, Beijing hasn't actively tried to overthrow current structures as much as it has worked to increase its influence within them. This may change as China's influence increases further. Beijing has made its position clear that is has little interest in U.S. dominance or adopting Western-style liberalism. Also, as one participant pointed out, many governments around the world don't perceive U.S. hegemony to be as benevolent as it is frequently framed in most Western countries. As another speaker argued, China's strong emphasis on sovereignty implies that any order China supports in the long term will most likely be firmly rooted in this concept.

Lea Gernemann, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Dr. Michael Hartlieb, Thomas-Morus-Academy Bensberg

Brigardier General Gerald Funke, Federal Ministry of Defence, Mischa Meier, University of Bonn, Colonel i.G. Sönke Marahrens, German Institute for Defense and Strategic Studies

At the same time, debates highlighted that the need to organize collective action for global common goods and to address shared threats is bound to remain a key element of global politics. In particular, participants pointed to the urgent need to establish new frameworks for cooperation to manage the use of the sea, space, and the cyber realm as well as the effects of climate change, and to mitigate the risks of escalating tensions between states. As power is shifting and states' abilities to reach their foreign policy goals alone is decreasing, power will likely have to be shared and existing structures will undergo transformations.

Overall, the wide range of different suggestions for what to expect from a rising China and how to proceed from a Western perspective – whether they were more realist recommendations focused on a combination of deterrence and dialogue or more liberal proposals based on enhancing cooperation and focusing on global commodities – revolved around the recognition that global structures need to be adapted to better reflect changing realities. While the exact path forward was contested among participants of the 2019 ISFB, the conference ended with a clear message: The key challenge for political leaders from all regions of the world is how to establish a long-term effective stability framework that all relevant actors are equally committed to. To be effective, such a framework will likely have to be based on as an updated system of norms for international behavior shared by all actors. One of the most crucial questions for international security may be how well China and the United States will be able to work together in addressing these challenges.

SPECIAL FOCUS DAY

Cyber Security and Artificial Intelligence

Key points

■ The world has not yet entered a fully digitalized era. Nevertheless, cyber already permeates virtually all areas of political and social life and is changing the rules and parameters of national and global governance, international conflict, and global security.

■ Due to rapidly evolving technologies, cyber is a moving frontier. Managing the cyber realm confronts policymakers with numerous new challenges, including blurring lines between war and peace, enormous difficulties in regulating and monitoring cyber activities, a proliferation of actors, and a considerable power imbalance vis-à-vis the private sector.

■ Cyber warfare and the development of AI are becoming a part of a larger global trend that revolves around increasing competition and weaponization.

■ Due to the unique characteristics of this only man-made domain, cyber warfare has an exceptionally low threshold for action and the potential for a dangerous upward spiral of retaliatory strikes with potentially devastating consequences that are often underestimated.

■ Despite the enormous difficulties that come with regulating and monitoring the cyber realm, the 2019 Special Focus Day showed a clear need for standards for cyber behavior and security by design to help contain these escalating dynamics.

Cybersecurity: Moving Frontiers and New Challenges

At the 2019 International Security Forum, the University of Bonn introduced a new feature: The Special Focus Day, a day reserved exclusively for the in-depth analysis of current trends in one specific field of international security. Presented by the Konrad Adenauer Foundation, the first Special Focus Day was dedicated to Cybersecurity and Artificial Intelligence.

At the beginning of the 2020s, the world has not yet arrived in a truly digital era. Despite the proliferation of gadgets and apps, the world is still largely analog, **Arne Schönbohm**, President of the German Federal Office for Information Security (BSI), pointed out during his welcoming remarks on October 2nd. With a view to artificial intelligence, the Forum illustrated that we are currently merely witnessing various levels of machine learning that are not equivalent to genuine artificial intelligence. However, debates revealed a clear consensus among experts that, if AI does at some point materialize, it is likely to become a true game changer for human society, politics and international affairs.

In any event, the impact of digitalization on human life is already enormous. From civil society and communications to critical infrastructures and political processes, the cyber sphere is expanding into virtually all aspects of life. As **Prof. Dr. Jürgen Rüttgers**, former Minister President of North Rhine-Westphalia and patron of the 2019 Special Focus Day, outlined in his address to the Forum, the enormous technological strides are also challenging traditional concepts and approaches to national and international governance, international politics and security.

In view of rapidly progressing digitalization of societies, economies, and politics, Bonn's Lord Mayor **Ashok-Alexander Sridharan** emphasized that securing these structures is becoming a key priority for policy makers. In terms of malware alone, the German Federal Office for Information Security identified approximately 800 million different malware programs in 2019. Taking note of the fundamental transformations to political and societal structures, the international United Nations City of Bonn is well on its way to becoming a leading center in cybersecurity, as the recent founding of the Bonn Cyber Security Cluster highlighted.

During the 2019 Special Focus Day, the complex issue of cybersecurity was approached from various angles: It was considered as a security issue, as a geopolitical issue, and as an issue of global public goods, with its various dimensions frequently overlapping. Throughout the discussions, it became clear that cybersecurity is as much a framing issue as it is a practical challenge.

Cybersecurity in an Age of Increasing Competition

During the 2019 ISFB, there seemed to be an overall consensus that the global community is living through an escalating dynamic that is marked by the resurgence of systemic rivalry between open democratic and authoritarian regimes, the reemergence of realistic thinking, and missing norms and rules for appropriate behavior. The cyber realm – including phenomena such as cyber warfare, the weaponization of data and social media, and the digital manipulation of political processes – is becoming a part of a dangerous trend that revolves around growing competition and overriding distrust.

Cyber Security Cluster Bonn e.V.
"The heart of cyber security in Europe"

The Cyber Security Cluster Bonn e.V. is a new institution that unites all relevant cybersecurity actors in Bonn. It was founded in 2018 and aims to turn Bonn into a European hub for cybersecurity by merging the strengths of public, academic and private sector players.

The 2019 ISFB highlighted a tendency among political observers and policymakers to transfer concepts from the analog into the digital sphere. One of the most common motifs in this regard is the propensity to describe what is happening between the United States, China, and Russia a "Digital Cold War." The Forum laid bare that many of these analogies paint a distorted picture that does not well represent the realities of an increasingly digital world.

From the Analog to the Digital

The differences between the cyber realm and other spheres are numerous. The Forum revealed that one of the key issues with cybersecurity is the fact that, due to rapidly evolving technologies, cyber is a moving frontier. As the only man-made domain, there are no natural laws in cyber space. Assessing the attributes of the cyber realm is much more difficult than those of traditional domains, obstructing the identification of possible threats as well as the development of sound solutions for its civil use and potential challenges and conflicts.

One issue that debates frequently circled back to was the observation that in an era that is marked by the expansion of cyber into all other spheres, the line between war and peace is starting to blur. Attacks in the cyber realm exist on a scale that may range from espionage to the weaponization of data and direct attacks against a nation's political integrity. Most of these fall into a grey zone of action that does not yet meet the threshold of what is traditionally considered an act of war. It was argued that the resulting ambiguity about what exactly constitutes an attack on a nation's sovereignty in cyber space, or even how the concept

of sovereignty should be applied to the cyber sphere, leads to a growing instability. In view of the blurring lines between peace and war, one participant quoted a British official's claim that today, "we're always at war," referring to Russian cyberattacks and similar issues. Various participants at the 2019 ISFB argued that the world has already entered a cyber war that is conducted below the threshold of open military intervention. According to one speaker, that war's first round "went to Putin, who defeated the U.S. without a shot being fired" by influencing the electoral outcome in his favor, deepening societal rifts, and destabilizing U.S. democracy.

As opposed to many other forms of warfare, the use of cyber is not restricted to states, enabling non-state actors or smaller states to execute attacks on a scale that used to be reserved for states with large resources. As technological advancements are empowering non-state actors such as terrorist organizations and even social movements as well as smaller states, the number of involved actors is increasing. With that, the world is entering an unprecedented situation that is unlike any example in history. While the 1900 battleship race saw around eight great powers struggling for dominance, for instance, and the 1960s were shaped by two great nuclear powers' competition for global hegemony, the world today sees the massive proliferation of a weapons technology with a very low threshold for action. According to different estimates, there are currently approximately 40 to 50 nations with cyber capabilities – not counting non-state actors. While it has been argued that this proliferation may cause a "democratization of conflict," a larger number of actors with cyber capabilities may also increase the potential for escalation.

left: Dr. Katharina
Kaesling,
University of Bonn

right:
Prof. Dr. Maximilian
Mayer, University
of Nottingham
Ningbo China

Another factor that shaped debates was that of transparency. Cyber capacities are much more diffused than traditional capacities. Due to the cyber space's unique characteristics, they are also significantly more difficult to measure and monitor, making it hard to verify another party's cyber capacities or track the source of a cyberattack. Combined, these factors keep the threshold for action in the cyber realm low. At the same time, discussions revealed that there seems to be little awareness among politicians and the public about what concrete implications an escalating cyber conflict might entail. The Forum illustrated a frequent inclination to divorce the digital from the physical world, which many IT experts considered a dangerous tendency. Against this backdrop, participants expressed their concern that the dangers that may result from states transferring their competition into the cyber sphere may fail to provide a disciplining effect on international affairs in a way similar to more traditional security challenges of the past.

The discussions highlighted that when it comes to cybersecurity, the stakes for societies are especially high. As digitalization extends into nearly all areas of life and from there back into the physical realm, cybersecurity needs be considered as a cross-dimensional issue. As opposed to traditional means of armed conflict, cyber warfare has the unique potential for an upward spiral of retaliatory strikes that may deeply affect critical infrastructure and political and societal systems. In light of this, the Forum disclosed serious concerns among experts that the current escalatory dynamics in international competition and cyber armament may point in a very dangerous direction.

Competition or Cooperation?

What became clear throughout the debates was that the approach to cyber is very different in Europe, the U.S., Russia, and China. The United States, China, and Russia each seem to approach cyber with a highly competitive mindset that is focused on identifying threats and developing comprehensive capabilities. China is leveraging its system of authoritarian state capitalism to create synergies between civil and military developments in the areas of technology and AI to boost development and production, and to accumulate massive amounts of data gathered by private companies.

With view to the EU, experts noted a different approach. For one, the EU's investments in cyber and AI are negligible when compared to China and the United States. While it was pointed out that some European states, in particular France, are internationally renowned for their excellent edge in research on AI, various experts maintained that the EU lags behind the U.S. and Asia in terms of technology development in a broader sense and also does not engage in close public-private research cooperation similar to that between the Pentagon and big U.S. tech companies. In recent years, the PRC demonstrated a striking jump in patent filings related to cybersecurity, including on AI, and has now surpassed all other regions in this regard, reflecting a geographical shift of innovation from west to east that leaves especially the EU outpaced.

In terms of security, the Forum showed growing fears that Europe's ambitious neighboring countries may be use the cyberspace to subvert EU member states' democratic systems: The evidence is mounting that Russia in particular is using non-direct attacks, interference and disinformation campaigns to widen societal cracks, create instability, and undermine trust in democracies' legitimacy – all of which fall in cyber's grey zone of action and retain the characteristic of deniability. Since around 2014, the continent has started to implement a wide array of countermeasures to cyberthreats, though so far, these have had moderate success. With view to the development of AI, one participant quoted Russian president Vladimir Putin from 2017, saying that "Artificial intelligence is the future. [...] Whoever becomes the leader in this sphere will become the ruler of the world." Current trends indicate that both China and Russia seem to be serious about the development and geopolitical use of cyber and AI. These attitudes raise a cardinal question: Does Europe need to take these assertions more seriously?

During the Forum, European officials emphasized that in terms of cybersecurity, the EU's focus is not on power competition, with various voices arguing that Western democracies should not enter in a cyber arms race. The EU vision is instead centered around two things: strengthening the bloc's security, especially through enhanced resilience and defense; and securing privacy and citizens' rights. The EU's declared aim is to focus on global commodities and a positive vision for cyber, as one participant laid out, in order to alleviate the competitive edge to cybersecurity.

Cyber and the Security Dilemma

Discussions during the Forum also turned to the observation that the extension of political conflicts into the cyber realm exacerbates some fundamental problems of international affairs and security. Cyber, one participant argued, has the potential to further aggravate issues known from peace and conflict studies and information processing research, which stipulate that conflict is seldom rational.

left:
Victoria Appelbe,
City of Bonn

right:
Dr. Enrico Fels,
CASSIS

*Prof. Dr. Jürgen Rüttgers,
Former Minister
President of North
Rhine-Westphalia*

Maybe most notably, this concerns the traditional security dilemma: Distrust of other states' intentions leads states to maximize their security measures. The inability to distinguish whether other states' actions are informed by offensive or defensive intentions results in the situation of the security dilemma: Misattribution of intent and worst-case thinking, which are especially prevalent in international conflicts, result in the danger of these becoming a self-fulfilling prophecy. Since both offensive and defensive cyber capabilities cannot be revealed due to their inherent logic and the cyber realm's general characteristics leave significantly more room for interpretation, these issues are heightened in a more digitalized era.

Privacy, Internet Governance, and the Private-Public Nexus

The 2019 ISFB highlighted another key aspect that is crucial to understanding the security implications of cyber: In the digital sphere, the private sector is now in the driver's seat. Cyber has heralded a shift in the private-public nexus. This concerns two different aspects: the development of national cyber capabilities as well as state's ability to regulate and monitor corporations' activities. States largely rely on access to private sector resources and know-how for the analysis of cyber threats and the development of cyber capacities for domestic and international use.

On the other hand, tech companies' irresponsible handling of user data may be turning into a serious threat to data privacy and ultimately contribute to undermining democracy, political stability, and basic liberties and rights. In both regards, the cyber sphere is marked by a significant resource imbalance between the private and public sector. As one participant pointed out, many tech companies' PR and other departments are bigger than some states' entire foreign policy institutions. This has serious implications for a state's capacities to effectively regulate and monitor private sector activity. At the same time, companies are gaining influence as an actor in global politics.

Due to this, a substantial portion of the debates revolved around the issue of internet governance and the framing of cybersecurity in terms of common goods. Debates underlined the clear need for political management of this realm, especially in terms of providing corporate activities with a framework, but also in balancing security with citizens' rights. In view of the difficulty that the enormous power imbalance between states and tech companies, experts at the Forum were divided regarding states' ability to effectively regulate and monitor the private sector's activities. However, one participant also noted a shift in the international perception of this issue, pointing out that the conversations among policymakers have largely already turned to the question of how to regulate the cyber realm instead of whether this is necessary at all. The real test will likely be the enforcement.

France has already been a forerunner in this regard: After dispatching a group of regulators to monitor Facebook facilities in Paris, Dublin, and Barcelona in early 2019, France has imposed legislation against online hate speech and initiated legislation for much more comprehensive legal directives, which the French government want to serve as model for EU-wide management of social networks. Several other countries have also introduced similar legislation. In fact, the European Union has become a driving force in this regard with initiatives such as the recent copyright directive. Participants seemed to broadly acknowledge that the EU can pave the way to data protection and assume a leading role in establishing international frameworks for internet governance, and is doing so already.

Prof. Dr. Wolfram Hilz,
University of Bonn

Prof. Dr. Yi Shen,
Fudan University

Dr. Sven Herpig, Stiftung Neue Verantwortung, Dr. Ulrike Franke, European Council on Foreign Relations, Goodarz Mahbobi, axxessio GmbH

Conclusion

The Special Focus Day saw a wide array of differing approaches and viewpoints on what implications the expansion of the cyber realm may have for security, stability, and citizens' rights. Depending on the framing – whether cybersecurity is considered as an issue of international security, as a geopolitical issue, or as an issue of public goods – the arguments as well as the specific conclusions may differ greatly. From the perspective of international security, the conference yielded one key result: The cyber sphere is becoming a part of a precarious trend in international relations that is characterized by escalating competition, distrust and a lack of norms for acceptable international behavior. The urgent question this raised is how the international community can start to manage and contain that trend.

Overall, experts at the Forum seemed split: A substantial group of participants maintained that the world has already entered a cyber arms race or even cyberwar below the threshold of traditional war, and that these are bound to intensify further. Multiple participants expressed doubts regarding the effectiveness of cyber diplomacy due to the host of unique characteristics that distinguish the cyber realm from other domains, including the difficulty surrounding the monitoring and enforcement of treaties and the

fact that traditional state-centric multilateral agreements don't account for the growing influence of non-state actors. Importantly, debates frequently circled back to the observation that the world is faced with a systemic issue that sees open democratic states pitted against authoritarian regimes, which are less likely to comply with international legal obligations. Furthermore, the growing emphasis on national sovereignty in many regions of the world may make it more difficult to establish norms and imply the need to manage expectations according to differing systemic preconditions.

As opposed to this, another large group of participants supported the view that both global governance and internet governance can be effective and are currently already contributing to providing stability to some extent. Many experts appeared cautiously optimistic that the odds of effective global governance in the cyber domain may in fact be fairly good if policymakers and governments adapt the lessons from previous arms control processes to the new preconditions of the cyber era. This may also mean underpinning legislative frameworks with a host of tailored technical solutions, such as developing a cross-national open source 5G system to bypass issues about who provides and controls this new technology.

In view of the devastating consequences that an escalating cyberwar may have, experts pointed out that the global community may be left with few genuine alternatives to establishing stable global frameworks. Various IT experts argued that there is no truly effective technical defense against cyberthreats, and that the unique potential for repeated retaliatory strikes may lead to political and societal disruptions of unprecedented dimensions. Combined, both of these factors thwart any expectations of reaching strategic stability. As one participant concluded, failing to rein in the expansion of international conflict into the cyber sphere may mean a "threat to civilization as we know it."

The debates at the 2019 ISFB revolved in large parts around the concept of "security by design." Though debates saw some skepticism among experts whether reaching this goal will be possible, they revealed the clear need for standards and norms to manage the cyber realm. To that end, it is key to better understand and communicate the extent of the possible consequences that may result from a failure to properly address cybersecurity challenges. It will also require political leaders to define more clearly what behaviors in the cyber realm are acceptable, what exactly constitutes an attack on a nation's sovereignty in cyber space, and what the responses to rule violations should be, as well as determining how to deal with non-state actors and defining the role of the private sector.

At the same time, debates also illustrated that any effort of establishing global frameworks to ensure lasting peace will be faced with the challenge of how to bridge the cultural gap and how to deal with systemic imbalances and differing preconditions between democratic and authoritarian states. One of these, one participant argued, is that the worst-case scenario for authoritarian states is regime change, while for Western democracies it is political degeneration and societal collapse, or what one participant described as "the return to the 1900s or even the Iron Age."

As a complex response to a global environment that is changing on a large scale, one speaker during the Forum laid out a theory for global governance in the cyber sphere, arguing that there may be a path to reaching it using a combination of measures based on the identification of common ground, setting rules of behavior, and establishing trust by implementing confidence building measures as well as mechanisms for rule enforcement. Following Alexander Wendt's Anarchy is what states make of it, one speaker concluded that in cyber space, the security dilemma may be what we make of it.

left: Dr. Alexander Klimburg, The Hague Centre for Strategic Studies

right: Lauren Zabierek and Prof. Dr. Dr. h.c. Karl Kaiser, both Belfer Center at Harvard's Kennedy School

SCENARIO
ROUND-TABLE
REPORT

Preparing for the Unknown

By Niklas Helwig and Alexandra Paulus

Early-career and senior experts gather on the first day of the International Security Forum to exchange ideas and thoughts on future security challenges. The discussion revolved around two concrete scenarios, which were selected from a large pool of applicants. How can Europe respond to a return of war to the Western Balkans? What happens if great power competition reaches cyberspace? The two scenarios described a not so distant future crisis with serious security implications for Europe and Germany. The exercise provided an excellent opportunity to think about the future trends in our security environment and what strategies and capabilities Europe needs for an appropriate response.

Each scenario was analyzed by two groups, one made up of young professionals and another one including the more experienced. All groups were made up of people with diverse backgrounds, including policy-

makers, the private sector, and academia. Since for each scenario, two diverse groups developed their analysis and response strategy, the results differed and covered different facets of the problems laid out in the scenario. This ensured lively debates and productive dialogue among the different groups.

The four facilitators, Jana Puglierin (German Council on Foreign Relations), Oliver Gnad (Bureau für Zeitgeschichte), Yixiang Xu (American Institute for Contemporary German Studies) and Carlo Masala (Bundeswehr University Munich) ensured a lively discussion. Niklas Helwig, who is a Senior Research Fellow at the Finnish Institute of International Affairs, and Alexandra Paulus, who currently pursues her PhD at Chemnitz University of Technology, provided the two scenarios.

left: Alexandra Paulus, Chemnitz University of Technology

right: Dr. Niklas Helwig, Finnish Institute of International Affairs in Helsinki

Strategic Foresight as a Method

Let us imagine a future scenario that holds the potential to change the security panorama for Germany and Europe drastically but which is currently deemed improbable. How would key actors probably react in this scenario? What might a strategic response look like? And what needs to be done today to prepare strategically for a similar scenario? These questions, in a nutshell, outline the method of strategic foresight. While an important part of strategic foresight is identifying trends and issues with growing relevance for future development, the aim is not so much arriving at predictions with total certainty. Instead, these exercises aim at identifying the key underlying factors, so-called drivers, that may enable the scenario in the first place. Examples of such drivers are technological innovations like machine learning or the rise of populist movements. Another key objective of strategic foresight is assessing which actions need to be taken to be better prepared for the scenarios that may, in one shape or another, come true one day.

At the scenario workshop, Carlo Masala encouraged the participants to structure their scenario analysis threefold: By analyzing, firstly, who is impacted by the scenario; secondly, what their interests are; and thirdly, developing a response strategy for Germany and Europe as a whole. This approach allowed for considering the different perspectives of all actors impacted by the scenario and identifying both common and diverging interests. The response strategies can point to blind spots or areas for improvement today, both for academics and policymakers.

Need for Strategic Foresight

One of the overall findings of the scenario roundtable was that Germany and its European partners need to develop capabilities for geostrategic assessment of trends and crises. Both scenarios showed a high number of actors with high stakes. Especially great power such as China, the US, and Russia played a crucial role in the European responses. Europe needs to understand the geostrategic interests of these international players and manage their relationships in a constructive manner.

The key actor is and remains the US. As the balance of global power shifts and the US is in the process of redefining its global role, uncertainty in the transatlantic partnership increases. It was therefore not a surprise that a great deal of thinking in the discussions focused on assessing the possible responses of Washington. While it was apparent that the US continues to have high stakes in the security of the European conti-

left: Ambassador (ret.) Dr. Volker Stanzel, German Institute for International and Security Affairs (SWP)

right: Dr. Dean Sheng, Heritage Foundation

The Benefits of Thinking the Unthinkable

Interestingly, the scenario workshop format was picked up during the conference plenary session in the context of debates on the relevance of political science as a discipline. Members of academia voiced their appreciation of the format because it allowed for out-of-the-box thinking. Uncommon or possibly inconvenient scenarios are addressed less in academic publications and discussions, to the detriment of academia's relevance: Unlike studies that reinforce generally held beliefs, drafting and analyzing scenarios that are, while improbable, possible might hold important lessons for both academics and policymakers. As recent development illustrated, the future may bring events formerly considered improbable. In that case, policymakers and academics would be wise to have prepared strategies for these formerly unthinkable scenarios that allow for more than just reactive policy.

To improve the format even further and bring the outcomes closer to this policy need, the group debated whether the format would benefit from a shorter time frame. Scenarios that are closer to the present might allow for more common ground for debate and strategic thinking among participants with very diverse backgrounds. Also, making the key drivers behind the scenario explicit might spark an even livelier debate.

In all, the scenario workshop demonstrated clearly that the format is relevant for academics and policymakers alike. The scenario choice also proved to be timely. Participants discussed the consequences of the return of violence to the Western Balkans at a time when Europe is struggling to formulate a coherent strategy for the region, while outside influence from Russia and China grows. The scenario on the fragmentation of the internet demonstrated the increasing intertwining of technology and security policy and the lack of strategic debate on an event considered likely by most participants. More exercises preparing the policy community to think the unthinkable are thus called for.

Scenario I:
War Returns to the Western Balkans

by Niklas Helwig

Scenario summary

The scenario describes a near future in which the multiethnic state of Bosnia Herzegovina disintegrates. Serb nationalists declare independence and found the independent Republika Srpska. At the same time, increasing ethnic tensions have led to the emergence of the Islamic State of Bosnia (ISOB). In late 2025, the terrorist organization attacks the government buildings of the breakaway state.

A number of outside factors drive these developments. In the run up to the crisis, the EU enlargement process on the Western Balkans stalls. The Russian leadership fans the flames of ethnic tensions with a disinformation campaign and by supporting Serbian nationalists. The United States, under the second term of Donald Trump's presidency, withdraws its engagement from the region. It is preoccupied with a growing conflict with Iran, which after the complete breakdown of the Iran nuclear deal follows an increasingly aggressive course in the Gulf region and beyond. Intelligence reports show that Iran is supporting Islamic terrorists on the Balkans and is behind an attempt to smuggle weapons into Bosnia Herzegovina.

As the ethnic tensions are rising in Bosnia Herzegovina, a tragic accident that kills a prominent Serbian family pushes the conflict over the brink. Serb nationalist use the public outcry to declare independence. ISOB announces its revenge and starts attacking the new Republika Srpska. "Nobody wanted this outcome, but today the Dayton agreements are all but dead and war might return to the Western Balkan," commented a veteran European diplomat, "like three decades ago, we don't know how to react. Just that this time the U.S. has no interest in helping us."

Situation assessment

The senior group identified three different threats to Europe, which determine the will and unity of the EU to respond. First, the drawing of new borders on the Western Balkans is troublesome, especially for member states with internal independence movements such as Spain. However, it might not be enough to spark a strong EU response. Second, the terror in Bosnia Herzegovina might prompt a reaction by Europeans, especially as it might result in large refugee movements. However, a local crisis might not be sufficient to create the unity behind a robust, even military European reaction. Third, the new and troublesome element of the scenario is the emergence of an Islamic state and the prospects of attacks in EU member states. This could be the red line to cause a strong reaction by the EU and its partners. The junior group made a similar assessment, but was much more confident that the first acts of terror in Bosnia Herzegovina would affect the security calculations of Europeans and prompt a stronger response.

A sizeable part of the discussion evolved around the question how regional and global players would react, in particular Turkey, China and the US. The groups compared Turkey's response to its role in the Syrian conflict, where it intervened to fight radical Islamists. China might have a substantial interest to contain the conflict because of its economic investments in the region. The big question mark for the participants was the possible response of the US. While the scenario suggest a limited interest of the US to get involved in Europe's backyard, the fight against terrorism and the influence of Iran might provide a stake in the conflict for Washington as well.

left: Austin Hudgens, Clearlake Capital Group and Prof. Dr. Carlo Masala, Bundeswehr University Munich

right: Michelle C. Watson, Cyber Intelligent Partners

Strategic response

The senior group was pessimistic about the potential role that the EU could play to contain or even solve the conflict. Already the scenario showed that the EU had lost influence on the Western Balkans in the years prior and remained divided when it came to a more robust engagement. A response would most likely focus on targeted sanctions and a monitoring mission that could stop the inflow of weapons. Only an ISOB terrorist attack in an EU country could convince the EU to go beyond containment of the crisis and authorize a NATO or EU military intervention. For that purpose, the EU would hope to get the US support as well.

The junior group was more confident about Europe's capability to go beyond containment of the conflict even without US. First, as none of the international actors, including Russia, has an interest in an Islamic terrorist state in the Western Balkans, the young par-

ticipants were confident to get the UN mandate for an anti-terror mission, followed by EU or UN troops to monitor the conflict. A naval mission would stop the inflow of weapons. Second, the military efforts would be complemented by a diplomatic initiative. A diplomatic conference in Oslo, would get a number of Western Balkan countries, plus Russia, Turkey, France and Germany on the table to find a post-conflict settlement of the border disputes and stabilize the region once more.

The two groups clearly assigned Europe different levels of ambition in solving the crisis. However, both groups agreed that the first step in the solution of a crisis on the Western Balkans is to understand the motives of the affected countries and manage Europe's often-difficult relations with them. Especially, Russia and Turkey were highlighted as important regional actors, which share the interest of a stable Western Balkans free of Islamic terrorism.

Key Takeaways

■ The ability of Germany and its European partners to contain, or even solve, a future conflict on the Western Balkans is limited. In the absence of major threats for European security, a strategy of containment is more likely than a military response.

■ Central to any response will be the relationship with major global and regional actors. A future conflict on the Western Balkans potentially affects economic and security interests of not only Turkey and Russia, but also China, Iran and Saudi Arabia.

■ It is conceivable that the US is not inclined to play a strong role in the solution of the conflict. Its commitment depends on the negative secondary effects of the conflict on US interests, such as terrorist threats, implications on Middle East balance of power, and great power relations with Russia and China.

Scenario II:
Fragmentation of the Internet

by Alexandra Paulus

The Scenario

By 2025, due to widespread ransomware attacks, attacks on critical infrastructure, and adversarial election meddling, global trust in the internet has eroded. The international community had sought to counter these challenges in a number of ways, but to no avail: Intergovernmental and private sector initiatives aimed at drafting international norms for responsible state behavior in cyberspace failed to create a consensus. Global economic entanglement was increasingly seen as an attack surface and thus reduced. The US doctrine of persistent engagement only lead to escalation and ultimately sparked a war between the US and Iran. And finally, the signaling of capabilities for deterrence purposes backfired, as it only increased the incentives for first strikes. Against this backdrop, a terrorist attack hits the SWIFT system, the backbone of international banking, not only provoking a major global economic crisis but also bringing citizens' and governments' trust in the internet to an all-time low. As a result, China is the first nation-state to publicly announce the roll-out of a national, completely independent internet. The threat of complete fragmentation of the internet, also termed splinternet, is looming large.

Anticipated Response

The senior group categorized the relevant actors and their anticipated responses along two axes: To what extent a fragmentation of the global internet would presumably negatively impact the actors, and to what extent they would have a vested interest in or presumably benefit from such an outcome.

They came to the conclusion that no one would be both highly impacted by and have a vested interest in fragmenting the internet. Most Western states including the EU and the US, in turn, would both be highly affected by fragmentation and have no vested interested in it, as would the academic community, banks, multinational companies, and individuals – as consumers, workers, and private citizens interested in open information and communication – because all of them benefit from open communication and transactions. However, internet service providers and providers of critical infrastructure would not be deeply affected by fragmentation but possibly benefit from higher earnings. And lastly, the group classified authoritarian states as neither deeply affected by nor interested in fragmentation due to their already limited exposure to an open internet. This sparked a heated debate, particularly when it came to classifying China, which different participants classified either in the first, third, or fourth category.

The junior group instead posited that all nation-states would primordially strive to maintain their sovereignty, security, and control over their territory. However, they also identified key differences between states, including between the EU and the US: While the EU would focus on the regulation of the internet, the US would stress economic freedoms, and Russia and China would emphasize control of information. Civil society and the Human Rights movement would stress the need for freedom of expressionand from

Marcel Stolz, University of Oxford

persecution, while the private sector would be most interested in economic freedom and market access.

The following debate centered around three key questions: Firstly, what would a fragmentation of the internet against the current geopolitical backdrop look like, considering the position of third countries and the dependencies created by China's Belt and Road Initiative – and how many fragmented internets would there be in the end? Secondly, the participants discussed how, in a splinternet world, certain channels for communication and transactions could be maintained open between rivaling internets. And finally, the role of proxy actors in cyber conflict in general and a splinternet scenario, in particular, received attention. Finally, consensus prevailed on the urgency of the discussion as many participants thought the scenario was likely and saw the danger of a slippery slope once one country starts building up their own independent version of the internet.

Envisaging a Strategy for the EU: Between Prevention and Mitigation

When it came to drafting a strategy for Germany and the EU, the ideas put forward had two different goals in mind: Preventing a fragmentation on the one hand, and mitigating its adverse effect on the other. Among the actions envisaged to prevent the laid-out scenario were diplomatic as well as educational and technological means. Firstly, the EU and like-minded states should forcefully maintain their goal of working towards an open, free, stable, and secure cyberspace and keep up their efforts, at the United Nations and

other for a, to draft internationally accepted norms of responsible state behavior in cyberspace in as inclusive a process as possible. At the same time, the diplomatic toolbox was seen asindispensable to prevent a vicious circle of pressure and reciprocity measures that may eventually, as a consequence unintended by all parties, lead to a fragmentation of the internet. Secondly, political education in all parts of the world was brought up as a cornerstone of augmenting societal resilience vis-à-vis related threats by third actors, such as information operations. And thirdly, participants discussed to what extent certifications and standards for products and information sharing between states, for instance,the disclosure of security exploits, may build up confidence and thus reduce the likelihood of fragmentation.

Participants who regarded a splinternet relatively inevitable focused instead on mitigation strategies. Some suggested creating a club of those states in favor of an open, free, stable, and secure cyberspace that could impose sanctions on others not abiding bytheir rules. Finally, discussions on industrial policy illustrated that it could serve a dual purpose: Fostering globally successful EU tech champions not only increases the EU's resilience in case of fragmentation but also makes such an outcome less likely by giving the EU more leverage vis-à-vis other states whose citizens use their products.

Interestingly, a matter that received next to no attention in the discussion – a stark contrast to the literature on the topic – was how states can increase the resilience of their administration, private sector, and citizens through fundamental cyber hygiene measures.

Key Takeaways

- Internet fragmentation appears highly likely because of policy disagreements within the transatlantic community and because authoritarian regimes as well as certain companies could benefit from fragmentation and might thus actively pursue it.

- A splinternet could be prevented through diplomatic dialogue, including norms building efforts, enhanced social resilience, and standards and information sharing.

- Faced with a splinternet scenario, states could mitigate its effects through sanctions.

- Industrial policy should be a priority since it serves both prevention and mitigation.

COMMENTS AND PERSPECTIVES

Russia, China, the Belt & Road Initiative and A New World Order

By Vladislav Belov

Dr. Vladislav Belov,
Research Director at
the Institute of Europe
of the Russian Academy
of Sciences, Moscow

At the end of 2019 we can see signs of obvious failures of global economics and policy: a return to international protectionism, the economic wars, Brexit, the Eurozone and migration crises, the rise of right-wing populism in Europe, the transatlantic fault/split, comparable economic dominance by China, the Arab Spring with its tragic consequences, Syria, the Middle East, the deepening disagreements between the great powers (the Russian-American and Chinese-American relations), a serious ongoing conflict in and around Ukraine, and the crises of arms control mechanisms. Any attempts to reform the United Nations invariably fall flat. The fragmentation of the international system, the gradual disintegration of the existing world order, and reduced manageability at the global and regional levels continue to affect every area of intergovernmental relations.

The world is close to the point of bifurcation, which will be followed either by the restoration of global governance at a new level, or by the accelerating slide of the world toward anarchy and chaos. The leading states and group of states are trying to promote various integration mechanisms and to create a platform for the shaping of the future world order, but they remain unable to reach any kind of common agreement on its restructuring. For a number of reasons, the traditional centers of world politics are unable to play a leading role in shaping the new world order.

The United States is in a situation of deep internal political division, and a long-term, balanced, and consistent foreign policy strategy cannot be expected from Washington in the near future. The European Union is grappling with a fundamental internal crisis and with a whole set of structural, financial, economic, and political crises. The EU is preoccupied by its many internal problems, rather than by the new world order. There are also difficulties with other leading players of world politics, objectively preventing them from taking on major responsibility for the formation of new rules of the game in the modern world.

One exception could be the most ambitious project in the world: "The Belt and Road Initiative" (BRI). China put it forward in 2013, when the international system had entered a period of instability. For six years now, the project has been one of the most important integration initiatives in the world.

The BRI is not only a huge economic initiative; it could also be considered an alternative approach to reformatting the world order "from below" – through the implementation of regional and continental projects envisaging the diverse and flexible formats for getting potential participants involved. The new China is not trying to build a closed club of states that do not like American leadership. This is a process of openness, inclusiveness, and joint development, not a closed bloc or a specific "Chinese club." The initiative does not divide the world by ideology and does not seek to play with zero sums. Any country can join the initiative if they wish to do so – the BRI is flexible and open for all participants, does not encroach on the fundamental principles of the liberal world order, and commits to continuing the process of globalization and beginning the process of reformatting the entire world order.

The BRI is in tune with Russia's integration efforts in the Eurasian space within the framework of the Eurasian Economic Union (EAEU). The pairing of these projects suggests that Moscow and Beijing are building new forms of world order, more effective than similar approaches in the West.

Not by accident, the United States, leading countries in the EU, India, and some other states are very critical and skeptical of the BRI, sensing a threat to their interests and their positions in the world, and have no constructive response to the implementation of the project.

Participating in the BRI gives countries a chance to develop their own projects and in this way to have an opportunity to lay down new rules of international cooperation together with China. Moscow understands that the changes to the world order through the BRI are just one example of the possible formats of building "from the bottom up" and of the creation of regional and continental coalitions of states that share common approaches to international interactions. From the Russian point of view, the BRI offers an opportunity to complement other entities. It was one of the reasons why Russian president Vladimir Putin welcomed the Initiative, noting that "combining the potentials of such integration formats as the EAEU, the BRI, the Shanghai Cooperation Organization (SCO), and the Association of Southeast Asian Nations (ASEAN) could become the basis for a greater Eurasian partnership."[1]

In this sense, Russia and China currently have significant advantages over other global power centers. They promote the idea of a "multipolar world" as the most sustainable, reliable, and fair design of a new type of international relations, which should be based on principles of mutual respect, justice, and mutually beneficial cooperation and build a community of one humanity, based on the equal participation of all countries in global governance, respect for international law, equal and indivisible security, mutual respect and consideration of each other's interests, non-confrontation, and contribution to a more just and rational polycentric world order.[2]

1   Igor Ivanov. The Belt and Road Initiative: Towards a New World Order. 05.06.2019. URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/the-belt-and-road-initiative-towards-a-new-world-order/
2   Joint Statement of the Russian Federation and the People's Republic of China on the development of comprehensive partnership and strategic cooperation entering a new era (in Russian). 05.06.2019. URL: http://www.kremlin.ru/supplement/5413

Therefore, Moscow and Beijing offer an alternative to the current world order, which is in a deep crisis. Of course, it's reasonable that this alternative can only be implemented in cooperation with other countries. The main advantage of the Russian-Chinese approach is that it is open to all participants, including the EU and the United States, in building a new configuration.

The multilateral mechanisms developed over the past two decades with the active participation of Russia and China (SCO, BRICS, EAEU) may eventually become separate components and elements of the future international structure. This structure should include the restoration of global governance, reform of the UN and other international institutions, a renewal of international law, and a new understanding of globalization and interdependence.

Russia is now defining its own long-term priorities and interests within the BRI project, taking into account its possibilities and limitations, and is ready to implement it as an indirect member of the project together with China and the other participants. The involved countries could find it easier to protect their own interests as part of flexible and fluid coalitions dealing with specific issues. Such a group of states may later form the coalitions needed to overcome the current crisis and form the future world order. Some expectations relate to the resurgent Russia-China-India triangle and new formats of EU interaction with Asian countries (the concept of transcontinental "connectivity").

The United States has no interest in forming a strategic partnership between the EU, China, India, other Asian partners, and Russia. Most likely, American policy will try to prevent it in every possible way.

The Eurasian projects of Russia (especially with China) have some advantages over its project with EU. The majority of Asian countries do not have many historical problems with Russia and negative stereotypes of Russia are less intense, with the Russian state not being seen as an existential threat – it is instead perceived as an attractive opportunity for economic expansion. The Eurasian project is still just beginning and the rules of the game/bureaucratic mechanisms have not yet been established. Russia can ensconce itself far more easily and simply in Eurasian processes on an equal-to-equal basis, and in certain areas even as a leader.[3] The project will involve different formats of Russian participation.

"Introducing" Russia into complex Eurasian transcontinental projects will require a high level of diplomatic skill, political flexibility, and readiness in many cases to play a "second role" to the leading roles of China, India, or ASEAN. Of course, justifying Moscow's meaningful participation in such projects will require a transformation of the Russian economy. The next five years will show how much the Kremlin will be able to solve this difficult problem.

3   Andrey Kortunov. Will Russia Return to Europe? 06.11.2018. URL: https://russiancouncil.ru/en/analytics-and-comments/
analytics/will-russia-return-to-europe/

In a Dissolving World Order, Europe and Germany Need a More Strategic Outlook

By James D. Bindenagel

Prof. James D. Bindenagel, Senior-Professor at CASSIS, Senior Non-Resident Fellow with the German Marshall Fund, former Henry-Kissinger-Professor (CISG), former U.S. Ambassador

With the power shift from U.S. global leadership to a bipolar world including a rising China, it looks like the jungle is returning to international relations, as Robert Kagan suggests. In this context, the question for Europe is whether it will choose the United States, its long-time partner, and the transatlantic relationship, or China, its long-time competitor and second-largest trading partner. And this at a moment when the perception that the United States is withdrawing from Europe has seriously damaged how Europeans see the country.

For example, public support for the transatlantic partnership in Germany is declining despite the seventy years of security and prosperity the transatlantic relationship has provided. According to the Körber Foundation, only 32 percent of Germans say the relationship between Germany and the United States is somewhat good. Nearly 52 percent are in favor of striving for more independence in defense matters. What is more, 50 percent say that there is a need for closer ties with the United States, while 24 percent advocate for closer ties with China and 18 percent are uncertain or see equidistance as an alternative.

At the same time, the days of European countries free riding on NATO security while promoting economic prosperity have ended. They must make a choice: in a climate of growing economic, political, and security challenges, Europe needs to decide whether to continue its dependence on the United States. The United States' re-evaluation of its alliances and commitments challenges European to take the torch to defend democracy in the transatlantic partnership.

Europe cannot lay claim to global leadership while relying on the United States for security. Can European countries muster the political will to reshape the transatlantic relationship and take responsibility for their own security? They have started addressing their deficit in military capabilities by strengthening their commitment to a common defense policy and by establishing new instruments of multilateral cooperation – including Permanent Structured Cooperation, the European Defense Fund, and the European Intervention Initiative. France is calling for strategic autonomy for Europe, including through the creation of a European army.

Other suggestions are being made. For example, Mark Leonard of the European Council on Foreign Relations proposes more "strategic sovereignty," in which EU member states exercise national sovereignty within a common European security policy. In this framework, individual countries could decide to meet their obligations toward a stronger EU alongside, rather autonomously from, the transatlantic partnership.

Such initiatives could make it possible for Europe to successfully execute a common foreign, security, and defense policy – and become more independent from the United States. EU law does not prevent member states from pursuing different security policies. But even though the initiative has been taken, there is no real debate about strategy in most EU member state, including the largest one.

For a More Strategic German Debate

The European Union and especially Germany – its most influential member economically and politically – need to find the political will to face the challenges of a dissolving world order. Member states must acknowledge the necessity of a long-lasting strategic debate in order to save the transatlantic relationship and the liberal values and stability of the European Union in a world that is succumbing to valuing "survival of the fittest" over cooperation.

It is unlikely that any meaningful debate on European security issues can be undertaken without Germany's support and political will. But it has to deal with several obstacles in this regard: a historical lack of strategic thinking, a troubled history, constitutional independence of the ministries within coalition governments, and public reluctance to support an international leadership role.

Germany's ambivalent response when the United States withdrew its troops from northern Syria was indicative. With no coordination with the foreign ministry, the conservative Defense Minister Annegret Kramp-Karrenbauer proposed a security zone with contributions by the Bundeswehr. The social democratic Foreign Minister Heiko Maas responded quickly with his own initiative that undercut the authority of

the defense ministry. His party stated that the defense minister's proposal was out of line. This shows how in a coalition government party politics can easily hinder a strategic debate, and makes the need for strategic foresight particularly clear.

Forming a Council on Strategic Foresight as an instrument of the parliament could foster the basis for a strategic debate in Germany. By discussing future scenarios and their implications as well as alternative actions before events have occurred, the tendency toward crisis management could be avoided and new possibilities opened up. This would create an atmosphere of action rather than reaction. At the same time, these debates would inform public opinion, influencing politics without encroaching on the policy-making process. A new German strategic culture, one that would focus on trends and their impacts on international politics, will be better able to anticipate concrete risks and opportunities and evaluate alternative options for policymakers.

Through such a council's reports on global trends, scenarios, and action plans, the parliament could contribute to an ongoing, informed public debate on strategy and foreign and security policy. Regular committee hearings on strategic foresight would also ensure a transparent and informed discussion of the challenges facing Germany and the policies best suited to meet them. Inviting representatives of allied countries to these hearings would further create crosscutting European ideas as well as build trust between Germany and European partners.

In the short term, the creation of a Council on Strategic Foresight would inform politics of critical issues and lead to a more informed policymaking process in Germany, assuring voters that important topics are being discussed in the parliament. In the long term, it could change the country's strategic culture into one that supports elites and politicians in conducting the necessary strategy for the country and Europe – either strengthening their values-based systemic partnership with the United States or fully rebuilding it.

This article has originally been published on the German Marshall Fund of the United States' website.

China, Europe, and Future Security

By Dean Cheng

*Dr. Dean Cheng,
Research Fellow for
Chinese Political and
Military Affairs at the
Heritage Foundation*

At the recent International Security Forum in Bonn, several analysts raised the idea that the European project, exemplified by the European Union, was intended to promote an alternative to traditional power politics.

Given the bloody history of the twentieth century, it is understandable why there is such interest in an alternative. But looming on the far side of the globe is a very different perspective, held by a civilization as old as Europe's – that of China.

While China has been described as more of a "civilizational state" than a "nation state," the bitter history of China's interaction with the West in the nineteenth and twentieth centuries has made China a fierce champion of national sovereignty. Indeed, there is arguably no greater defender of the Westphalian international order than the People's Republic of China (PRC).

It is therefore ironic that, even as Europe strives to downplay nationalism and move toward a trans-nationalist or post-nationalist order, China warmly embraces nationalism. Indeed, Beijing is clearly intent on defending its rights as a nation state, whether in terms of its territorial sovereignty (including its claims to Taiwan, Tibet, and Xinjiang), or its rights in the new spheres of outer space and the Internet.

This divergence in perspective is reinforced by the divergence in approach. Europe is committed to a rules-based order, in line with its longstanding commitment to the rule of law. China, by contrast, has never developed a rule of law perspective throughout its five millennia-long history. Instead, it has generally viewed the law as an instrument to support previously established political goals; this is rule-by-law, rather than rule-of-law. Coupled with Chinese economic capability (as the second-largest economy in the world) and growing technological prowess, China poses a growing challenge to the European and Western approaches to international behavior.

This growing friction is displayed in the Chinese disregard for intellectual property, in its efforts to circumvent restrictions on its access to advanced technology, and its treatment of information flow and access. This pattern of behavior reflects a broader point: that China is unlike most past challengers to the international system.

Whether Napoleon, imperial Germany, or the Soviet Union, past revisionist powers have tended to rely more on military capability. In the case of the PRC, the main tool seems to be much more economic and informational. Indeed, because of the Chinese Communist Party's assessment that the twenty-first century has seen the rise of the Information Age, wherein the ability to generate, analyze, and transmit information more rapidly and more accurately than one's competitors, information has become the focal point of national development. It is no accident that China has focused on developing information-related technologies, or has systematically sought out others' intellectual property, i.e., information on embryonic technologies. They see information as the lifeblood of this new age.

This is not to suggest that China has neglected the development of its military. The recent Chinese National Day parade displayed a range of capabilities from unmanned aerial vehicles to fighter jets to advanced missiles. Nor is that military only for parades; Chinese naval forces have recently engaged in exercises in the Baltic and Mediterranean for the first time in recorded history.

But the foremost tools China has thus far relied on are more in the realm of economics, whether Belt and Road Initiative investments or large-scale purchases of raw materials, and in the realm of political pressure, often expressed through non-traditional means such as Confucius Institutes. The type of challenge China poses is very different from those that Europe, or the United States, has confronted in the past century.

It is therefore essential for national security analysts and thinkers, such as those associated with the International Security Forum, to adopt a fresh outlook and approach. Just as China is not the Soviet Union and the world does not face a rerun of the Cold War, it would be a mistake to rely on past precedent, be it containment or arms control, to deal with this returning power. While longstanding concerns about sovereignty, nationalism, and deterrence remain central, how they are expressed in the economic as well as military realms, especially in light of advances in information and space technology, will be ever more salient.

The challenge of a revived China, something not seen in several centuries, cannot be answered with old approaches, but demands new thinking if other nations are to be up to the task of meeting it.

A New Challenge: Climate Security
The Geopolitical Implications of Climate Change

By Friedbert Pflüger and Arash Duero

left:
Prof. Dr. Friedbert Pflüger, Director of the European Centre for Climate, Energy and Resource Security (EUCERS), Department of War Studies, King's College London, and managing partner of Pflüger International GmbH

right:
Arash Duero, Senior Fellow at the European Centre for Climate, Energy and Research Security (EUCERS), Department of War Studies, King's College London, and Advisor to the World Energy Council's Global Gas Centre.

After the Russian-Ukrainian gas crisis of 2009, energy supply security was pretty much on top of the European Union's energy agenda, which ultimately culminated in pursuing a cohesive strategy of "Energy Union" in 2015. Since then, the EU has markedly improved its energy security situation. Now, another challenge – a more universal one – is emerging that must be urgently addressed: climate security, that is, mitigating and managing the geopolitical implications of climate change. Unfortunately, this challenge has not been given the attention it warrants. Indeed, climate change has become a threat multiplier that is exacerbating volatile situations around the world with dire geopolitical implications.[1]

For many, climate change poses an existential threat, while for others, at least in the short term, it can become an advantage. Just one flashpoint to consider is the Arctic and Greenland.

The Arctic and Greenland

Rising global temperatures are melting our polar ice caps. Over the last three decades, the Artic has experienced some of the most rapid climate changes on Earth, almost twice the global average. As ice fields, glaciers, and sea ice continue to melt, countries are increasingly recognizing their potential to unlock vast tracts of natural resources like oil, natural gas, and minerals. The Arctic accounts for about 13 percent of undiscovered oil and 30 percent of undiscovered gas.[2]

The opening up of the Northeast, Northwest, and other passages due to the melting ice gives rise to new questions about who has the right to control seaways or exploit vast undiscovered natural deposits. These questions raise serious geopolitical concerns, and rightly so, given the history of tensions in the region between the five Arctic coastal states (Canada, Denmark, Norway, Russia, United States), as well as other actors like NATO and China.

The U.S.' Renewed Interest

Recently, President Trump played with the idea of buying Greenland. While his proposal elicited global astonishment and widespread ridicule, it was, in fact, not a completely outlandish idea. Greenland has long been important militarily given its key position between Russia and North America. In 1940, the U.S. seized control of Greenland to prevent the island from being used as a springboard for an invasion of North America. During the Cold War, Greenland's strategic geographic location was used by the United States to track Soviet submarines and place bombers and later missiles that could attack enemy targets, as well as position missile early warning radars at the American air base in Thule. Today, Greenland remains as important as ever for the United States and NATO, particularly in light of Russia's enhanced military capabilities and China's growing economic clout.[3]

Russia's Enhanced Military Capabilities

In 2007, Russia staked its claim to Arctic territory by planting its flag on the North Pole seabed. Fast forward to 2019, and its interest in the region has only grown. In November 2019, Russia conducted a major military exercise in the Arctic involving 12,000 soldiers, five nuclear submarines, fifteen warships, and 100 aircraft, as well as the launch of the world's first "combat icebreaker."[4] Moreover, it has five nuclear-powered icebreakers, currently the only country to have any, and is also upgrading its military installations at its northernmost airbase in Nagurskoye,[5] which will give Moscow advanced capabilities to defend its territory and the ability to strike Thule Air Base, the U.S. Air Force's northernmost base, and thus cause significant damage to its missile defense and early warning systems. In geopolitical terms, Russia's increased activities in the Arctic have two key aims: 1) to gain a strategic military position with strike and defense capabilities against potential adversaries in the region and 2) to bolster Russia's claim to around 1.3 million square kilometers of the Arctic.

China's Growing Economic Clout

The opening up of the Arctic has also become of interest to countries not usually associated with the region. In its 2018 white paper, China launched its Polar Silk Road Initiative, which aligns Beijing's Arctic interests with the Belt and Road Initiative. In the paper, China describes itself as a "Near-Arctic State" and makes it clear that it has a strategic interest in being involved in natural resource extraction as well as commercial activities, including shipping.

Already, China has sought to project its economic influence through commercial forays in Greenland. A Chinese state-owned company has invested in a rare earth elements (REE) and uranium mining project at Kvanefjeld in southern Greenland,[6] while another Chinese investment company has expressed interested in purchasing a former naval station.[7] In 2017, the Chinese government applied for permission to build a satellite receiving station. As trade starts to pick up with the melting ice opening up the seaways, it is likely that China will attempt to increase investments in the region. Eventually, Chinese capital could make up a significant share of the island's economy, giving Beijing leverage that could be used to pursue not only commercial, but also geopolitical interests.

For instance, if China decides to develop major infrastructure along the Polar Silk Road, it will warrant close attention. Such facilities could easily be re-purposed for military use with strike capabilities against both the United States and Russia, a significant development at a time when the U.S. is reducing its international engagements while Beijing simultaneously seeks to be recognized as a major power with a growing global reach.

Conclusion

Whether in discussions about melting ice, rising temperatures, or extreme and unpredictable weather patterns, links are being made between a changing climate and geopolitical developments. And it is truly a global problem. Emissions produced in the United States lead to melting the icecaps in the Arctic, which in turn is detrimental to Pacific island states and has security and economic implications for the five Arctic coastal states and beyond. As the manifestations of climate change increase and become more extreme, their effects will play an increasingly important role in discussions of security and geopolitics.

Although these challenges represent a relatively new field, comprehensive strategies need to be developed to respond to climate-induced security threats and geopolitical instability both nationally and around the world. The Paris Agreement is a good first step in pushing us to commit to curbing emissions and drafting climate adaptation action plans. But pledges and promises alone are not enough. We need to step up and turn them into concrete action.

Artificial Intelligence, 5G, and Geopolitics

By Benjamin Fricke

Benjamin Fricke, Policy Advisor for Transatlantic Relations at Konrad Adenauer Stiftung

Artificial Intelligence (AI) is the term generally applied to the process whereby computer algorithms analyze and apply huge amounts of data to the point where machines can "learn" on their own. AI is clearly becoming one of the most significant and defining technological developments of the twenty-first century. The next industrial revolution triggered by AI and enabled by 5G will profoundly change our human interactions. 5G will enable exponentially faster download and upload speeds, as well as providing significantly reduced latency for numerous devices, while allowing wireless networks to communicate with each other.

Whether through changes in global supply chains and transportation systems (autonomous cars), medical technology breakthroughs (remote surgeries), social control mechanisms, or the way modern-day warfare is conducted, 5G will become the basis of a new global communications architecture upon which AI will be applied and through which the Internet of Everything (IoE) will become the backbone of our societies. This change in technological modernization will not come without challenges and consequences for the U.S.-led world order that has endured for the last seventy-five years.

Indeed, artificial Intelligence, 5G and quantum computing will profoundly change our global politics. These technologies will become the most important emerging advancements in the next ten to twenty years. Our current world order is already challenged by rising powers that possess these technologies, and it is crucial for Germany and the EU to improve their global competitiveness and tap into the vast potential of AI, 5G, and big data. Geopolitical and economic supremacy will be determined by those powers who successfully implement and utilize manage AI and 5G.

China has explicitly documented that by 2049 it plans to become the world's premier global superpower, surpassing the United States. Through China's enthusiasm for some aspects of markets and profits, its implementation of a prolific and systemic theft of intellectual property (IP) worldwide, a decades-long forced transfer of knowledge from outsourcing, and their own extraordinary hard work, hundreds of millions of Chinese citizens have achieved middle-class status or better. This transformation appears to many as a counter-model to the U.S.-guaranteed liberal democratic western world order. China's Hundred-Year Marathon is aimed at replacing the U.S.-led world

order with alternative economic and digital networks, while simultaneously building up a military presence in places such as the South China Sea and the Indo-Pacific. Essentially, China is combining the geopolitical theories of Alfred Thayer Mahan and Halford Mackinder into one national global strategy: sea power vs. land power.

The Russian approach, in contrast to the Chinese, is more focused on the military applications of AI. Russia has not only announced the development and production of the Avangard (a hypersonic glide vehicle), capable of actively avoiding radar and point defense system detection and delivering nuclear and conventional payloads, but it has also developed a nuclear-powered cruise missile called 9M730 Burevestnik, capable of carrying thermonuclear warheads. The Russian Federation is working on AI to create swarms of drones ready to be used on future battlefields.

The most advanced cyber and AI players today are the United States, Russia, China, and to a lesser extent, the European Union. Large tech companies, however, are mainly located in the United States and China, while Russia is primarily focused on military and government efforts.

The small number of companies capable of producing and implementing 5G technologies suggests a highly-competitive international market with significant barriers to entry. National and regional players, such as Germany and the EU, could start forming a more independent industry and build up AI capabilities at home to protect their societies' open character, but there is also the critical question of maintaining national security. The application of AI and other key emerging information and communications technologies will be a critical defining factor for the success of nation states and alliances in the future.

All in all, AI and 5G will become the most important emerging technologies within the next ten to twenty years, with the potential to fundamentally alter the global balance of power. Moreover, geopolitical and economic supremacy will be determined by those powers who manage AI and 5G to their advantage. Russia and China are already challenging the U.S.-led world order by providing new technological competition. Lastly, Germany and the EU are lagging behind in both 5G and AI adaptation. Their global competitiveness will continue to decline unless they invest in EU-based technology-capable companies that can manage big data and exploit the seemingly limitless opportunities such data offers.

A Technical Forum for Confidence-Building in the Autonomous Weapons Realm

By Malte Göttsche

Prof. Dr. Malte Göttsche, Leader of the Nuclear Verification and Disarmament Group at the Aachen Institute for Advanced Study in Computational Engineering Science (AICES) Graduate School of RWTH Aachen University

Today, we find ourselves in a world of diminished trust among global actors, one characterized by power competition and a qualitative nuclear arms race. Against this background, research and development efforts that contribute to enabling autonomous weapon systems (AWS) are particularly worrisome, as such efforts may aid the initiation of yet another technological arms race. Preventing this requires confidence-building, to which not only the policy, but the scientific community should also contribute.

Autonomous Weapon Systems

No consensus exists about the definition of AWS. A key characteristic is that these systems could autonomously select and engage targets. They "will be able to operate without human control or supervision in dynamic, unstructured, open environments [...]."[1] However, it is hard to define a threshold, as the degree of autonomy is a spectrum.

The use of AWS may not be far in the future. Prototypes are being tested in several countries, and several precursors already exist. The current main competitors in this field are the United States, Russia, and China. AWS may offer advantages to the military: fewer soldiers would need to directly engage in combat. In the absence of the human need for rest, endurance during warfare would be enhanced. Reaction times would be reduced if systems did not require a remote soldier to make decisions. Individual communication links that can jam would no longer be required. Weapon swarms would become possible.

However, the risks ultimately outweigh the benefits. AWS would reduce predictability and control on the battlefield. Given the impossibility of training the control program for all possible circumstances in combat, potentially grave mistakes could occur. Other limitations include that artificial intelligence will in the foreseeable future not be able to reliably distinguish between combatants and non-combatants. This inability, along with quick response times, could cause conflicts to almost instantaneously escalate.

Regulating AWS

States may be tempted to invest vast resources to develop AWS, either to be the leaders of the development, or to avoid falling behind. While there could be temporary military advantages, there seem to be no long-term benefits of such an arms race. Instead, it would increase the probability of war, including by erroneous decisions of AWS.

1   Altmann, Sauer, Survival 59, 2017

These risks should be an incentive to regulate AWS. There are ongoing discussions in the Group of Governmental Experts in the context of the Convention on Certain Conventional Weapons in Geneva. At least thirty states propose to ban their development, deployment, or use. However, those states investing in relevant research object to banning AWS. If consensus is required, as is the case under the current format, a ban is unlikely. Germany seeks a middle ground by proposing to formally declare that all weapon systems must be undergirded by meaningful human control.

Overall, the discussions are highly controversial and, at best, slowly evolving. So what are additional options to seek progress?

Scientific Contributions to the Debate

The history of nuclear and chemical arms control shows the importance of integrating scientists into the discussions. In particular, the Nuclear Non-Proliferation Treaty, most bilateral United States-Russia nuclear arms control agreements, and the Chemical Weapons Convention have strong verification regimes whose development depended crucially on scientific expertise. In the case of the Comprehensive Test Ban Treaty, it was the Group of Scientific Experts that helped pave the way by developing the verification approach of the treaty many years before it was finally negotiated.

Technical work also acts as a confidence-building measure, as the currently active International Partnership for Nuclear Disarmament Verification demonstrates. At a time when nuclear disarmament is a highly divisive issue, this group nevertheless successfully discusses how it could be verified and conducts exercises. The participating countries, who hold diverse views on nuclear disarmament, do so by not spelling out how it could be achieved politically. Indeed, a success factor of the Partnership is that it is more a technical than a political forum. Besides diplomats, technical experts also participate, including academics. This enables them to achieve concrete scientific results.

How could a technical forum of interested parties be an avenue for progress in the AWS context? Here, the debate is much less framed than in nuclear disarmament discussions, which have a legal basis in the Non-Proliferation Treaty. A verification regime as part of an arms control treaty will likely not be the first step in preventing or limiting AWS.

A technical forum could build confidence by preparing the ground for future voluntary transparency initiatives. For example, it could develop technical approach-enabling exercises in which states could demonstrate that during certain tests of weapon systems, no autonomous modes were explored.

How to Assess the Non-Use of AWS?

Since it is unlikely that direct participation in such exercises would be possible for reasons of sensitivity, there is no simple way to establish the non-use of AWS. Also, there are no clear characteristics that could be identified upon observing the actions of a weapon system, for instance via video, to prove that it is acting or has acted autonomously. Even with the ability to fully examine software and hardware – a highly unlikely scenario – it would be hard or even impossible to reach a conclusion: the same hardware could be used with or without autonomous mode, and the authentication of complex software is extremely challenging, sometimes impossible.

Even though it was developed for the arms control verification context, a cryptographic method could provide a way forward through voluntary demonstrations that prove the actions of a weapon system are the result of orders given by humans.[2] According to this concept, human-machine interactions would be recorded in an encrypted database. When asked for proof that a specific weapon system did not act autonomously during a specific event observed on video, the state could make available the particular records.

This is only a preliminary idea; much more work will be required to develop it, and perhaps also different and approaches can be thought of. The focus of the proposed forum should be on technical dialogue. Only when a certain level of trust has been built through this process can actual exercises be discussed.

In conclusion, as consensus in Geneva is far from emerging, other avenues should be explored, and new actors should be engaged in the debate. The scientific community has an important role to play, as it can contribute to building confidence and generate new and innovative ideas.

2   Gubrud, Altmann, Compliance Measures for an Autonomous Weapons Convention, ICRAC, 2013

Competing Compasses in the Post-Cold War Era

By Jackson Janes

Dr. Jackson Janes,
Senior fellow at the
German Marshall Fund
and president emeritus of
the American Institute for
Contemporary German
Studies (AICGS) at Johns
Hopkins University in
Washington, D.C.

Thirty years after the end of the Cold War, transatlantic relations are entering another era, yet without a name and without much consensus about what to expect. The post-Cold War era began with a great deal of hubris on both sides of the Atlantic with labels like the "end of history," but now it seems to be ending with more sober approaches to the next chapter of challenges to global security. What will be the description of the post post-Cold War period? Some have suggested a few: The Era of illusions, The Age of Anxiety, The Return of Realism. Whatever the name, the environment of this era will be shaped by forces we know but also don't yet know.

Following World War II, the United States held sway over the globe as the most powerful country in the world, producing over half of the world's GDP and possessing the only nuclear weapon capability until the Soviet Union established itself as a nuclear power. Today the US makes up less than 20 percent of global GDP, is no longer uncontested militarily, and is challenged by alternative political approaches.

After climbing out of the ashes of war, the process of rebuilding Europe took place in a divided Europe and required building bridges over both physical and psychological barriers. Today, the EU is comprised of 27 members with a total of 450 million citizens, around 15 percent of global GDP and some of the highest standards of living in the world. Yet there are serious centrifugal forces pulling at its fabric that have led to Brexit, populist blowback, economic asymmetries and political grievances, not to mention foreign policy challenges that remain unmet.

These developments have led many to question the survival of what is commonly referred to as the "West": a model of political, economic, and social organization that had been championed as the future of a liberal global order. But that version has been challenged by other versions emerging elsewhere around the globe questioning many assumptions made in the wake of the fall of the Berlin Wall: the ultimate efficiency of liberal democracy, the necessity of a global market for capitalism, and the increasing need for international governance in an interdependent world. The increasing polarization within the so-called Western democracies is undermining their capacity to develop a consensus to confront new challenges.

In 2020, a century after the disaster of one world war which was to lay the foundations for another just two decades later, the temptation to draw parallels is pervasive. What did those who had just seen the worst demonstration of mass killing on the fields of Europe miss in developing tools to avoid an even worse version? Are we missing our warnings now, made manifest in the centrifugal forces of nationalism, economic disparities, fear, and hubris, which provide the opportunity for demagogues to manipulate all of it?

In contrast, we might ask what warnings were heeded after 1945 and how, in the aftermath of World War II, they enabled one part of the world to emerge with tools to forge a more lasting set of institutions, goals, and alliances designed to sustain a partially peaceful world as a model. Part of that answer was in the leadership supplied by the United States which committed itself – this time – to providing the resources to sustain those efforts, build the organizations, and enforce the rules. Another part was the commitment of partners to work together on shared goals. The Cold War was still a war, and there was a shared threat that motivated collaboration. But it was about more than avoiding war. It was about what the larger world we share might look like if we worked within a framework of common interests and aspirations.

But after 1990, while many thought that we had been successful in getting things right after over four decades of Cold War, we were quickly reminded that we should never take things for granted; history was not quite finished, and we still had a lot to learn from it. In the wake of the disintegration of Yugoslavia, the return of war to the European continent in the Balkans was one of many red flags pointing at the fact that the melting of Cold War ice sheets had uncovered the fires

of nationalist entities. The brutal suppression of human rights demonstrations in the streets of Beijing in 1989 should also have reminded us that a global convergence of values was not self-evident. The turmoil in Afghanistan did not subside after Soviet troops left, but continued to simmer until it boiled over a decade later in the attacks of Al-Qaeda in Africa – and then on 9/11 in the US. Regional conflicts continued, financial insecurities erupted, inequalities deepened, and the bonds of alliances were increasingly strained. As Reinhold Niebuhr has written, "The course of history cannot be coerced in accordance with a particular conception of its end."

As we prepare ourselves for this next era, our past milestones can assist in showing us from whence we came, but where we are headed will be dependent on the assumptions we make about our challenges and the choices we make in confronting them. In the coming decade, there will be competitive models showing how to respond to climate change, worldwide migration, the role of government and the rules of governance, and the responsibilities of citizens and nations to each other. There will also be competing visions of strategic security. That environment will involve multiple levels of power, not shaped in a bipolar or unipolar framework but in a world that is multi-dimensional in terms of interests and ideology. There will be asymmetries of influence, resources, and ambitions.

In that world, what will be the basis for stability? Looking back to 1945, the capacity and willingness to share goals was inspired by the catastrophic impact of war, the confrontation with the Soviet Union, and a shared set of political values. That was the same basis for the creation of the EU. In 1990, the hope that this shared framework would expand even further globally was symbolized by the fall of walls. Yet during the next decades, we were reminded that we are not done with the debate about the evolution of our various visions of modernity. Engaging in that debate requires inclusion of a larger scope of issues about the nature of international security and the parameters of governance we need to secure it. That has been the mandate of CISG, now part of CASSIS at the University of Bonn.

As Neil MacGregor has said, "the idea of community is to embrace not only those who share our beliefs but also who share our world. 'Who are we' is the greatest political question of our time." Whatever the next era is to be called, this question will remain pivotal.

Looking Ahead

By Karl Kaiser

Prof. Dr. Dr. h.c. Karl Kaiser, Senior Associate of the Transatlantic Initiative at the Belfer Center's Future of Diplomacy Project and Adjunct Professor for Public Policy Emeritus at the Harvard Kennedy School

If one reviews the state of global politics looking at where the most pressing problems lie, four stand out: the breakdown of arms control, the climate crisis, the erosion of multilateralism, and ensuring that China's rise remains peaceful.

The withdrawal of the United States and Russia from the INF Agreement signals more than an end to the prohibition of intermediate nuclear weapons. It signals the end of an era, terminating the practice and habit of nuclear cooperation between these adversaries that helped to preserve nuclear peace. President Trump's disruptive and anti-arms control policy has actually been more important than Russia's violation of the agreement's terms in producing this break-down. To be sure, his administration's argument that the growing nuclear arsenal of China must be dealt with is entirely valid, but to use the solution of an inherently difficult problem as a pretext to discontinue a working agreement undermines the basis of nuclear stability. The same is true for the extension of the New START Treaty on strategic weapons beyond February 2021. Despite Russia's willingness to renew the treaty without preconditions, the Trump administration has been reluctant to do so, pointing to the necessity of

dealing with China's potential. A dialogue on nuclear arms control with China is, indeed, necessary, but its uncertain outcome should not block a treaty between the globe's two biggest nuclear powers and thereby potentially unleash a resumption of the arms race in strategic weapons. The European governments should use all their available influence inside and outside of NATO to induce both powers to resume their nuclear arms control.

As the climate crisis intensifies and progresses, it will profoundly change global politics, though many of its consequences are unpredictable. It is nevertheless foreseeable that the increase in global climate temper-ature will further strain already struggling economies, eventually causing some to collapse. It will instigate conflicts over scarce resources (most notably water), unleash vast migration pressures (particularly on Europe because of the neighboring Broader Middle East and Africa), make large areas unhabitable, and necessitate massive transfers of people and of coastal cities with the rise of sea levels. Practically every coun-try on the globe will suffer – though some more than others – but will this induce cooperative or conflictual behavior, common solutions, or a nationalistic sauve

qui peut using all the instruments of the state, including the military? Whatever the outcome may be, it is evident that only a dramatic change of policy to fight climate change can alleviate the crisis and thereby improve the chance for global peace. The EU's "Green Deal" is a step in that direction; it will hopefully be implemented and induce other major actors to follow suit.

The postwar multilateral order is being eroded at various levels, most consequentially in a significant part of the world economy. The main responsibility lies with the Trump administration and its "America First" policy that applies bilateralism and protectionism in its trade policies, imposes tariffs unilaterally, and is de facto destroying the World Trade Organization by blocking its dispute mechanism. But the role of China, which likes to pose as a defender of multilateralism, should also be mentioned, since it has consistently violated basic rules of fair trade with its subsidization of state firms, forced transfer of technology, and theft of intellectual property. In this respect, the European Union, which itself stands for the realization of the most advanced version of multilateralism in the form of integration, has a particular responsibility to uphold the principles of multilateralism as the core of a liberal trading order. It will hopefully continue not only to directly resist the Trump administration's protectionism but also "circumvent" the United States with a series of global trade deals that implement proven principles of multilateralism, such as its agreements with Canada, Mercosur, or Japan.

Finally, China's rise will restructure international politics and make the American-Chinese rivalry the central feature of the future international system. Whether that rivalry will lead to military conflict is entirely open, but the management of that relationship will no doubt be crucial for global stability during the rest of this century. China's expansionist territorial policy, notably in the South China Sea, does not bode well in this respect, nor does the authoritarian nature of the regime. At this stage, the EU enjoys a flourishing economic relationship with China. It nonetheless has economic and diplomatic problems with China as it faces the Belt and Road Initiative, with its implied aim of creating dependence, as well as China's "17+1-policy," which attempts to create division inside the EU. But an escalation of the U.S.-Chinese security rivalry to a military conflict would inevitably affect Europe as well and in many ways. It is therefore in Europe's profound interest to contribute wherever it can to maintaining peace in East Asia.

A Challenge for IT Security Experts: Small and Medium Enterprises and Industry 4.0

By Goodarz Mahbobi

Goodarz Mahbobi, CEO at the IT and management consultancy axxessio GmbH in Bonn and Darmstadt

Digitization is moving forward at a rapid pace – it affects society and economy, countries and cities, as well as large companies and small and midsize enterprises. Bigger players usually have enough resources to deal with the consequences of the digital transformation; however, for smaller players often-times this is not the case. Moreover, they need to use their limited resources to adapt even more fundamentally.

In 2015, Ashok-Alexander Sridharan, Lord Mayor of Bonn, and I started the initiative "Digital Bonn" to motivate involved parties in government and business in the region to take on a more strategic approach to digital transformation. One of the first plans implemented was the foundation of the "Cyber Security Cluster Bonn" for the Bonn/Rhein-Sieg region to set up an "army of the good." This has been a major milestone for the initiative due to IT security's critical role in new digital processes. Although IT security is a base requirement, even the IT industry itself still has some large blind spots in this area. So do cities and SMEs – but they cannot simply deal with this by spending large amounts of money. They need a different approach.

To gain a better understanding of the situation, we took a closer look at the state of IT security in Germany's industrial SMEs. German SMEs are extremely successful; still, the digitization of the industrial sector and the improvement of IT security present a major challenge to them. To overcome this potential disruption and keep its status as one of the leading industrial nations, Germany has developed an "Industry 4.0" strategy. Industry 4.0 requires the integration of digitalized assets with communication networks – hence, IT security becomes a critical factor for its success.

While the perceived importance of IT security among SMEs is generally high and increases with company size, there still is a great discrepancy between perception and action. This is indicated by the small pro-portion of SMEs that have actually carried out an IT security analysis.[1]

This lack of action can be linked to SMEs' lack of empowerment regarding IT security, which has been confirmed by various surveys. In summary, SMEs would like to understand the IT security problem better – but there is a need for better information; trust-worthy external IT-security consulting; training; better, more user-friendly security software; and standardized IT security measures.[1]

1   A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, und I. Henseler-Unger, „Aktuelle Lage der IT-Sicherheit in KMU".
    WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, 2017.

Missing this kind of support, decision-makers in SMEs do not ignore the problem but turn to sources of information they trust. In Germany, they primarily rely on their social network of other companies to search for information, exchange ideas, and discuss problems in closed forums.[2] However, by relying on familiar social networks and not turning to new sources of information, the situation stagnates and IT security awareness cannot be improved. This was particularly evident in the development of planned investments in IT security between 2011 and 2017: more companies invested in IT security, but the overall level of investment did not increase. Above all, the biggest problem is the 54 percent of companies that either have no investments planned or answered "they don't know" in response to a question about whether they are planning new investments.[1]

The question remains regarding what measures could increase the investment in IT security among SMEs at this point in time. Surveys show that for SMEs, the greatest influence on investment in IT security is exerted by regulatory requirements, digital transformation, and customer requirements. Regulatory re-quirements are powerful since they affect all competitors equally. Digital transformation investments always come along with IT security investments since these form an important basis for digitization. Fi-nally, customers can exert great pressure on SMEs to meet their requirements, which are at this time often linked to Industry 4.0 projects. Other incentives for IT security investments are strategic business orientation, industry standards, and recent media coverage of cyberattacks. Surprisingly, surveys found that current security incidents in one's own company or within an industry have the smallest impact, compared to the aforementioned reasons.[3]

Industry 4.0 can play a significant role in IT security awareness: 76 percent of managers expect an increased IT security risk to accompany Industry 4.0 investments.[2] Therefore, companies active in the In-dustry 4.0 sector attribute greater importance to IT security and more frequently perform IT security analyses. They are forced to deal intensively with their processes and data, which leads to a better under-

standing of their assets. Moreover, they assign higher significance to their assets and data protection. This is reflected in the survey results of "Industry 4.0 companies" compared to companies not active in the field of Industry 4.0: the need for data protection for R&D data doubled, rose about 8 percent for process data, and increased by 15 percent for machine data.[1]

Clearly, Industry 4.0 has a positive impact on SMEs' IT security activities. At the same time, however, data protection and data security requirements are still seen as the biggest barriers for the implementa-tion of Industry 4.0 itself.[4] The development of Industry 4.0 and IT security are heavily interdependent; they can boost or inhibit each other.

Oftentimes IT security is not taken into account right from the start. Subsequent changes are always expensive and sometimes impossible. Still, we have seen that overall interest to invest in existing pro-jects is low – new, well-planned IT projects, especially in the field of Industry 4.0, can boost the motiva-tion to take IT security seriously. Furthermore, the IT security sector can support SMEs' efforts in Indus-try 4.0 by better understanding the requirements they are trying to fulfill. These are often a result of market competi-tion: 60 percent of surveyed companies responded to be in a cost and quality competition and 31 percent to be in a time and innovation competition.[5] It is of crucial importance that the IT security industry adapts its offers to the needs, the competitive situation, and the IT security obstacles of SMEs. Only in this way can SMEs keep up with development.

2   „Cyber Security Report 2018 Teil 2: Unternehmen – das Risikobewusstsein sinkt". Deloitte, 2018.
3   P. Engemann, D. Fischer, B. Gosdzik, T. Koller, und N. Moore, „Im Visier der Cyber-Gangster So gefährdet ist die Informationssicherheit im deutschen Mittelstand". PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC), 2017.
4   A. Berg, „Industrie 4.0 – Wo steht Deutschland?" bitkom, 2018.
5   „Industrie 4.0 im Mittelstand". Deloitte, 2016.

Huawei and Europe's Strategic Autonomy

By Sönke Marahrens

Col i.G. Sönke Marahrens, Colonel (GS) and Program Director of the German Institute for Defense and Strategic Studies

During the panel discussion on European technological autonomy, the audience witnessedswitness a vivid discussion between U.S. and Chinese participants regarding the issue of Huawei's control of 5G technology and its planned application as the base for 5G networks worldwide. The U.S. participants accused China of using its technology monopoly to gain control over the Internet infrastructure of their clients. The Chinese participants countered the allegations by reminding the audience that Huawei has answered all requests for information and provided all the information asked for by governments worldwide. They tried to shift the discussion to a point of challenging the United States by arguing that, first, U.S. IT businesses cannot provide state of the art 5G technology; and second, that the accusations are part of an economic war conducted by the actual U.S. administration in order to protect the weaker U.S. IT companies – an act which China considers a violation of international trade laws.

The European participants followed the discussion very intently, adding insider and technical knowledge and questioning both positions, but finally sided with neither the United States nor China: "At the end, we can only choose who will spy on us."

The underlying security politics problem runs much deeper: it is far beyond a choice of technology; it is a discussion about whether and how Europe and/or Germany will or can maintain decision sovereignty.

The actual U.S. government approach of tolling and using national laws to target international competitors is hitting European market participants directly and indirectly. EU producers therefore can be targeted either directly for their market share in the United States or for future technological superiority over U.S. products, as exemplified by China. That, or they might become collateral damage of U.S. national economic actions – like the German auto industry, when the United States hit Mexico and Canada in order to revise the NAFTA agreement. Although China has proven that the actual 5G technology is coming without a backdoor, a simple remote-controlled update might change this, as history has already proven. From a European perspective, U.S. tech companies could be accused of this as well.

The heart of the issue is that outsourcing or loosening technical independence in essential technology fields like mobile internet, artificial intelligence, or computing will lead to European and German dependency on others, possibly preventing Europe from thriving.

In a world in which rule-based behavior is constantly being contested by autocrats and the autocratic tendencies of democratically elected governments worldwide, strategic decision autonomy is highly dependent on a secure and available IT infrastructure. Maintaining this strategic decision-making autonomy requires stringent holistic and critical analysis and a common understanding of critical IT infrastructures. Critical infrastructure must be understood in all dimensions. Undisturbed and uninfluenced internet access to control national or European CRITIS is as important as the provision of life-essential power supplies or water.

Therefore, future European and German security strategies must claim national/European decision-making autonomy equally in order to respond to today's common issues of protecting their territory and their citizens. It must be understood that the rise of regional hegemons like Russia and China is challenging the existing world order and that, currently, even the creators of the Bretton Woods system prefer nationalism over international trade. Living in a volatile world requires the willingness to break old paradigms rather than insisting on maintaining the status quo in the face of actors unwilling to step back or down.

Future security strategies must be (re-)expanded by aspects of diplomacy, cyber, and economics in order to cover all changes, chances, threats, and challenges. To cope with the unreliable behavior of allies as well as the hegemonic actions of China and Russia, the society and population must be prepared to confront this behavior. European states must decide on how they want to shape the future – actively or passively. This requires investment, R&D funding, and a clear understanding of the dynamics of international politics.

Artificial Intelligence in the European Union: Choosing the Right Path

By Nicolas Mazzucchi

Dr. Nicolas Mazzucchi, Research Fellow at the Fondation pour la Recherche Stratégique (FRS) in charge of cyber, energy, and primary goods issues

Artificial intelligence (AI) has been defined by Marvin Minsky as, "the science of making machines do things that would require intelligence if done by men." AI could be considered a game-changer in most activities as it would address most human activities when mature. In the military, the use of AI could be considered not only an enhancer but a strategic leap, as these technologies would complement the work of soldiers and experts. AI-based technologies could be present from the HQ to the forefront of the battlefield. As a consequence, the race for AI is open between major powers. Considering this framework, the European Union (EU) must enter the competition for AI with its specific areas of interests, according to its own goals.

AI: From Buzzword to Strategic Issue

At present time, AI remains mostly an in-development family of technologies. Very few genuine AI applications are available, especially in the military, and those are mostly based on connectionist technologies making an extensive use of data to achieve a proper result. Moreover, on-the-market AI solutions mostly use structured data making them of little use for the military. Having an autonomous vehicle that can only follow routes with road signs is a problem for vehicles intended to be used off-road in the desert.

Nevertheless, the most promising AI-based technologies, which provide support to the decision-maker, would revolve around symbolic AI, which is currently under-developed. Because developers, from GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) and other major companies remain focused on technologies that can be quickly released to the market, amount of funding on symbolic AI appears limited. Here is a clear opportunity for public and private spending to complement one another, allowing research and development to achieve the convergence of symbolic-connectionist AI.

The position of EU countries regarding the development of AI-based technologies appears to be far behind the two superpowers: China and the United States. As demonstrated by the number of patents and the figures on public and private investment on AI, there is a gap that seems impossible to fill, unless EU policymakers can clearly decide on supporting specific technologies. Alongside this issue, the EU has to choose how it seeks to regulate AI-based technologies in the military at a global level, including technological and industrial forums.

A Follow-Up of EU Global Orientation on Cyber Issues

AI is a cyber-based family of technologies and relies mostly on two elements: computer processing capabilities and availability of data. As the technology gap between European industries and U.S. or Chinese industries is widening, the risk of a technical lag of Europe in AI is high. As Europe did not encourage the rise of major data processing companies, following a competitive path on pure computation power or data management seems to be unrealistic. Nevertheless, the EU has not been inactive on cyber issues and technologies, adopting regulations on the use and security of cyberspace and data for years.

Regarding the three pillars of information management – availability, integrity, and confidentiality – the European Union made the choice to focus on confidentiality. The recent European regulations on data and cybersecurity emphasize this choice, as both the Network and Information Security (NIS) directive and the General Data Protection Regulation (GDPR) are focused on protecting the privacy of European citizens. The extension from a cybersecurity policy dependent on critical infrastructure operators to one based on data and information providers is a major evolution of Europe toward the protection of Europe and its citizens.

GDPR especially is considered a first attempt for the EU to implement a regulation with extra-territorial consequences. Having the upper hand on the confidentiality of data helps the administrations to control the use of European data by private companies.

Which Technologies to Focus On?

As a consequence of EU strategic orientations on both cyber issues – especially regarding data and the development of military technologies under European Defense Agency or Permanent Structured Cooperation (PESCO) – EU policymakers are taking a deep look at AI solutions. Armed forces all over Europe, especially France and Germany, are considering the use of AI-based technologies to enhance their operations and limit the gap with major non-EU military powers. According to national strategic documents, these technologies may be used in nearly all military functions, from intelligence to cybersecurity or predictive maintenance. Nevertheless, with this wide area of application, there is the need to focus on specific technology issues to avoid the inefficient "spreading" of investments, especially with national priority divergences.

To be coherent with prior policy positions, it seems that the EU should focus on AI explicability, as this is a major issue. Explicability is an important feature for the training of AI with a wide variety of data to achieve a certain agility of the system. These AI technologies could provide both agility and sturdiness for the systems they would equip, especially considering the possibility of deceiving or jamming the recognition patterns. As the US DARPA is doing with several research programs, the EU – through the European Defense Fund – should have a clear focus on this strategic issue.

Second, the EU should also focus on the certification of AI results. As some military AI would be used on the battlefield, the need to ensure that the results of AI processing are not corrupted is a major concern. In terms of cybersecurity products, the EU and most of the member states have been able to ban non-compliant products from Europe. This policy could be extended to AI-based technologies, requiring a European body of AI scientists to evaluate the compliance of various technologies. This ex-post strategy appears to be the most adequate balancing of past EU cyber policy and the limits of European military industries. This specific orientation would also manifest a specific European position at the global level regarding AI technologies in the military, charting a third way between the interdiction of autonomous systems and their unrestricted use.

A Fatal Neglect: On the Significance of U.S. Soft Power Today

By Hendrik W. Ohnesorge

Dr. Hendrik W. Ohnesorge, Managing Assistant and Research Fellow at the Center for Global Studies and Chair in International Relations at the University of Bonn

In modern times, U.S. presidential campaign slogans have become a crucial hallmark for what to expect from an incoming administration. Bill Clinton's "It's the Economy, Stupid!", for example, famously encapsulated the president's promise to focus on economic reform and recovery after the end of the Cold War. In a way, such slogans are, of course, vastly oversimplifying, and their effective explanatory power may be limited in a world of complex challenges. Still, they offer a glimpse into the mind and worldview of a candidate or, if elected, president, and provide insight into a (prospective) administration's setting of priorities – both with respect to its ends and its means.

This holds particularly true for the incumbent in the White House, Donald J. Trump, and his campaign slogan "Make America Great Again" ("MAGA"). The centrality of the slogan was expressed not least in Trump's inaugural address, the last words of which repeatedly echoed the mantra. After inauguration, the catch-phrase did not lose any of its significance. On the contrary, not only have the "MAGA" caps sported by Trump supporters become an omnipresent reminder of the slogan, the official webpages of the White House also frequently utilize varieties of it. For Trump himself, as indicated in a January 2017 interview with The Washington Post, the emphasis in his quest for "Making America Great Again" lies in a restoration and, if possible, increase of its hard power, exemplified by the president's references to "jobs," "industry," and "military strength."[1] The U.S.-China trade war, economic sanctions slapped on a variety of actors, the surge in military spending, and the establishment of the United States Space Force are but a few, if arguably among the most striking, expressions of this decided focus on hard power. A crucial dimension of power fatally neglected by the Trump administration, however, is that of soft power.

---

1   Quoted in Karen Tumulty, "How Donald Trump Came up With 'Make America Great Again'," The Washington Post, January 18, 2017, online at: https://www.washingtonpost.com/politics/how-donald-trump-came-up-with-make-america-great-again/2017/01/17/fb6acf5e-dbf7-11e6-ad42-f3375f271c9c_story.html (January 10, 2020).

Whereas the former rests upon military and/or economic coercion, the latter draws upon the forces of attraction in international relations. In Joseph S. Nye's definition, soft power thus refers to "the ability to get what you want through attraction rather than coercion or payments."[2] In this context, culture, values, policies, and personalities can be potent sources of soft power, which frequently even eclipse those of great armaments or economic prowess, as countless examples in the long annals of international relations prove.[3]

To date, however, the Trump administration has indicated as much disdain for attractive soft power as it has displayed a proclivity toward the coercive instruments of hard power. Whether it is the slow (or even still absent) filling of crucial posts in the state department, major cutbacks in relevant agencies and programs, the termination of various international treaties, or the scorn toward traditional multilateral fora, Washington seems to disregard the tools of soft power to a degree seldom, if ever, witnessed before. Its public diplomacy, crucial for conveying one's message to an international audience and understanding foreign perceptions, is in dire straits today as well. What is

more, an unprecedentedly blunt rhetoric, a high degree of political volatility, and major changes of course have unsettled friend and foe alike. Taken together, these trends have delivered a considerable blow to U.S. credibility, a crucial currency of soft power. Consequently, observers like Stephen M. Walt have already identified the downsides of what Walt called the administration's "bullying approach" to foreign affairs.[4]

In a world facing rising or revisionist powers and vast security challenges ranging from climate change to nuclear proliferation to international terrorism to cyber threats, the forces of attraction are of vital importance. Of course, military and economic power continue to loom large in international affairs. The neglect of the instruments of soft power, however, comes at a considerable price. A president who has set out to "Make America Great Again," therefore, would do well to take them into consideration. This observation becomes all the more glaring given that a major part of America's historical international clout has sprung from its prodigious soft power.

2   Joseph S. Nye, Jr., Soft Power: The Means to Success in World Politics (New York: PublicAffairs, 2004), p. x.
3   Hendrik W. Ohnesorge, Soft Power: The Forces of Attraction in International Relations (Cham: Springer International Publishing, 2020).
4   Stephen M. Walt, "America Isn't as Powerful as It Thinks It Is," Foreign Policy, April 26, 2019, online at: https://foreignpolicy.com/2019/04/26/america-isnt-as-powerful-as-it-thinks-it-is/ (January 10, 2020).

Tough Choices Ahead for European Security

By Benjamin Rhode

Dr. Benjamin Rhode, Senior Fellow for Transatlantic Affairs and Editor of The Adelphi Series at the International Institute for Strategic Studies (IISS). The views expressed here are his own.

The International Security Forum convened by the Center for Advanced Security, Strategic, and Integrations Studies and the American Institute for Contemporary German Studies in early October 2019 featured several important discussions concerning the role of the European Union and its constituent states in a world increasingly marked by the exercise of "hard power," and whether the EU's non-military strengths could serve as a substitute for its continuing ineffectiveness in the military domain. One participant employed an imaginative and thought-provoking paleontological metaphor: while the EU was, in essence, a herbivore dinosaur, could it make itself sufficiently large and intimidating, as the brontosaurus did, so that it could remain secure in a world dominated by carnivores? Unfortunately, Europe's continued security in recent decades has not been a result of its development of a novel paradigm in which it is able to fend off or deter predators despite being largely ineffective as a military actor. Rather, it has in practice been guarded by an extremely potent carnivore – the United States – which is now in the process of resiling from its former commitments.

Since the Forum took place, several events have confirmed the pressing nature of these questions and the predicament in which European states find themselves. Ongoing revelations about U.S. president Donald Trump's dealings with Ukraine suggested that he was willing to jeopardize the security of a European partner – albeit one that was not a NATO member – in the hope of securing its assistance in a defamatory campaign against a domestic political opponent. In the Middle East, Trump's abrupt withdrawal of U.S. forces from northern Syria highlighted his administration's determination to shed itself of existing military commitments, whether or not this involved the abandonment of its allies. While they did not suffer the catastrophic consequences experienced by America's Kurdish partners, Trump's announcement caught Washington's European allies off guard. Moreover, Turkey's invasion of Syria shortly afterward illustrated and exacerbated longstanding divisions within NATO. During tensions between the United States and Iran in January 2020, which many feared could produce a major conflagration, the extent to which European states had little to no meaningful influence over events that affected their national interests was striking. More generally, U.S. policy toward Iran since 2018 and the collapse of the JCPOA have demonstrated the futility of European states' hopes that they could pursue an independent policy toward Tehran.

Trump's startling announcement of the U.S. withdrawal from Syria was one of several challenges to NATO that French president Emmanuel Macron discussed in his interview with The Economist in autumn 2019. While this interview attracted widespread coverage – and a fair amount of indignation at Macron's outspoken remarks, especially that NATO was "brain dead" – it is noteworthy that many critiques focused less on the substance of Macron's commentary and more on its apparent indiscretion. Macron's ominous prognostications about the future of NATO's Article V were condemned for themselves undermining NATO's credibility; yet he was reflecting broadly held concerns over whether the Trump administration would honor its commitments to defend European allies, heightened by Trump's open musings over whether Washington would protect states such as Montenegro.

In his dealings with allies in the Middle East and Asia, President Trump has repeatedly demonstrated a narrow interpretation of the national interest, typically identified in financial terms. For example, he has repeatedly threatened to withdraw U.S. forces from Japan and South Korea unless those states increase their financial payments to Washington dramatically; and he has recently claimed that the United States has received large payments from Middle Eastern allies in return for military protection. Whether these claims are in fact correct, these declarations are illustrative of a firmly-held worldview that scorns traditional alliances, and they validate concerns voiced privately and publicly by European states about the extent to which they can continue to depend on the United States for their security. Events over the past six months or so, moreover, have undermined the consoling narrative that President Trump's alarming announcements were mediated by his officials and could for the most part be safely ignored. Trump has repeatedly demonstrated that his views are the primary determinant of U.S. foreign policy, with officials scrambling to create post hoc rationalizations for his often-impulsive decisions.

Although their diminishing global influence is increasingly apparent, European states have not experienced a direct and severe threat to their security since Trump's accession to the presidency. That would change were Trump to announce Washington's withdrawal from NATO. It has been widely reported that aides had to dissuade him from doing so at his 2019 State of the Union address. There remains a strong possibility that in 2020 the president will both be acquitted of impeachment charges and re-elected to the presidency, which he would interpret as validation and legitimization of his policies at home and abroad. It is likely that a second Trump administration would continue to retrench from Washington's global commitments and undermine traditional alliances – but much more dramatically than before. While the U.S. Congress has sought to employ legislative means to forestall American withdrawal from NATO without its approval, the stubborn fact remains that a presidential declaration that Washington would not respond to an invocation of Article V with military support would itself deal a devastating blow to the Alliance's credibility.

European states are well-aware of the scale of the threat that these developments pose to their security. The UK defense secretary has recently made public his concerns that London's assumption since at least 2010 that any future war involving British forces would see them fighting alongside U.S. allies may be misplaced. Paris and Berlin are also conscious of the changing strategic landscape shaped by U.S. retrenchment. Yet there remains an apparent division between the views of Macron and his advisors that Trump represents a broader shift in U.S. attitudes requiring a commensurately dramatic European response, and the implicit hopes of many within German diplomatic and political circles that, were a Democrat to defeat Trump in the 2020 election, the figurative storm would pass, and they could return to the comfortable status quo ante in which Washington bore the cost and responsibility for defending Europe. Events over the next year or so may reveal which of these assumptions are correct.

AI and Warfare: Pending Issues for Europe

By Kaan Sahin

Kaan Sahin, Research Fellow for Technology and Foreign Policy at the German Council on Foreign Relations (DGAP)

Advances in artificial intelligence (AI) will impact and permeate most aspects of life, and the military and security domain are not exempt from these progressions. AI holds great potential for warfare to be waged in a faster, more precise, and 'less human' fashion with new enhanced capabilities. Faster, because AI systems can process large-scale data and make decisions for military operations based on that; more precise, since machine-learning enabled tools such as object and facial recognition as well as foresight analyses promise, in theory, superior accuracy; and 'less human' as decision-making powers are transferred to machines – be it in terms of anticipating or mitigating crises or even in battlefield situations.

Concerning the development of potential new capabilities, the international debate (especially in Europe und Germany) on how AI is transforming the battlefield is predominantly focused on the development of lethal autonomous weapons systems (LAWS) or – in a more plastic visualization – 'killer robots' and how to stop or contain these developments. It is to some extent understandable that a particular focus is on AI-enabled capabilities with the biggest possible 'nightmare scenarios'. However, as indicated above, AI in the military context goes beyond LAWS. The potential application possibilities comprise several fields, including cyber and information operations, logistics, data and

intelligence gathering, the enhancement of command and control capabilities, and unmanned naval, aerial, or land-based vehicles.

This poses enormous challenges for armed forces such as, among others, the question of how to incorporate this wide variety of AI-enabled systems into the strategic, operational, and tactical planning and implementation. Furthermore, the implications of becoming more reliant on machines in the military realm must be addressed from the technical, political, and ethical side.

A Shift in the Public-Private Nexus

However, not only the tools or the way warfare is conducted are subject to change, but there is also a shift concerning the sources of technological developments, including relevant defense technologies. The source of technological innovations is now the private sector in the first place, which is manifested in how the market value of great tech-companies such as Google, Amazon, Baidu, and Alibaba have increased over the last years.

This has profound implications for governments in general which are becoming more and more reliant on private companies. In other words, this entails a shift

in the public-private nexus. For instance, the two so-called AI superpowers – the United States and China – have increased the collaboration between their militaries and commercial enterprises in recent years. In the U.S. case, the Pentagon and DARPA (Defense Advanced Research Projects Agency) as its main R&D entity is pushing for collaborations with big tech companies in the framework of Project Maven to integrate AI systems into the military realm. And China is developing the so-called state-led 'military-civil fusion' to produce dual-use technology systems such as AI and better integrate and transform commercial developments into their armed forces.

Given this geopolitical context, the EU and its member states are trailing behind in the development of most of the emerging technologies such as AI. The militaries and the defense sectors are affected by these developments.

Recent Activities on National and EU Level

These new emerging parameters pose a series of questions. The EU is under pressure to find solutions and approaches to cope with the growing significance of AI in the military. Yet, initial approaches and developments toward that direction can be identified lately.

First, European states have started to draft AI-related military documents: In September 2019, the French defense ministry published its first AI military strategy. It is hardly surprising that Paris took the initiative in that context since the French AI strategy (For a meaningful artificial intelligence) from March 2018 already emphasized the need for the creation of synergies of civil and military technological innovations to develop AI capabilities in the security realm. Also, in Germany, where the defense community has been rather timid in acknowledging the military AI dimension (beyond arms control matters) in the past, the German Army Concepts and Capabilities Development Centre released a position paper on AI use for land forces one month later.

Second, those developments are flanked by recent initiatives on the EU level. In August 2019, AI was on the agenda of an informal meeting of EU defense ministers, whereas Finland has further pushed the issue during its presidency of the Council of the EU in the second half of 2019. Beforehand, in May 2019, Finland, Estonia, the Netherlands, Germany, and France issued

as food for thought "Digitalization and Artificial Intelligence in Defense", which is a good point of reference for the current status of the EU in this realm: Although it presents a good overview about how the drafters perceive the issue, it is salient that the paper's prime purpose is to pose unanswered questions.

Challenges Ahead for Europe

Broadly speaking, three areas for action for the EU and its member states can be identified: First, in order to achieve a productive transfer and adaptability of commercial AI technology for military purposes in European context – as trivial as it may sound – a strong AI industry in Europe in the long term is an essential prerequisite, with the need of more investments. Since AI is a general-purpose technology, the development of an AI ecosystem on the European level will benefit all kinds of areas and industries, including militaries and the defense sector. For instance, advances in image recognition algorithms for non-military intents can also be modified for object identification in combat situations. Furthermore, to increase AI-related defense research and in order to materialize the notion of a European innovation system, more joint laboratories and research partnerships are needed to facilitate closer research between the military, the defense industry, commercial enterprises, and academic institutions.

Second, since the EU itself and its member states are still very much in the early stages concerning the interface of AI and warfare, a fundamental analysis about the current status of AI military integration in the member states must be carried out. This will help to point out the gaps and identify how to pool and develop AI-related capabilities in order to boost cooperation in the field of AI among the member states. The European Defense Fund can play an important role in this context.

Third, in order to achieve a thriving AI defense ecosystem on a European scale, the EU and its member states have to set regulatory framework conditions and show the political will to include AI in the European security context beyond ethical arms control discussions.

In sum, Europe is at the beginning of the process of integrating AI technologies into the military realm. However, considering the global developments, the need to act is pressing.

The Challenge of Digitalisation – the Bundeswehr Cyber and Information Domain Service

By Jürgen Setzer

GenMaj Jürgen Setzer, Vice Chief of the Cyber- and Information Domain Service and Chief Information Security Officer of the Bundeswehr

Digitalisation offers tremendous opportunities for science, economy, government and civil society and thus for each and every one of us living in democratic and liberal societies.

At the same time, however, it also provides enormous opportunities for potential enemies – be they criminals, terrorists or state actors – and thus involves considerable dangers to our society. The possibilities of digitalisation have given rise to a new form of conflict, for which we need to prepare. Cyber attacks on states and their critical infrastructure as well as business enterprises and private households have already become reality. From a technical point of view, future conflict scenarios will be characterised by digitalisation, artificial intelligence and automation.

Besides attacks from cyberspace, activities intended to manipulate or influence opinion, such as fake news campaigns and disinformation, have become all too common. Therefore, the inclusion of the information domain is of particular importance. Consequently, both cyber and information space are of vital importance when it comes to national security and thus the military.

As early as 2016, at the summit in Warsaw, NATO recognised cyberspace as a military domain in its own right – much like the domains of land, air, sea and space. Armed forces can both reconnoitre and engage enemy systems in cyberspace. In practical terms, this could involve, for example, the interruption of logistic chains or the modification of data crucial to enemy operations. Paralysing C2 and information systems would also be an option.

In the Bundeswehr, we have deliberately chosen a broader definition of this new military dimension – one that includes the above-mentioned information domain as well as its central aspect: information. Information is perceived, interpreted and disseminated by human beings. Hence, what is called "published opinion" constitutes an essential part of the information domain.

The new cyber and information domain is characterised by a high level of complexity. Territoriality is complemented by virtual reality. Cyber and information space cannot be divided into traditional combat sectors with clear spatial boundaries.

Contrary to classic kinetic operations, cyber operations can also achieve the desired effects by non-lethal means or for a limited period of time. Nevertheless, physical effects can be achieved in cyberspace, too. Moreover, the place where cyber operations create an effect can theoretically be tens of thousands of kilometres away from where the action was initiated. Time, too, plays a different role in cyber and information space. An effect can be achieved over any distance almost without delay. Hence, effects are achieved in real time.

Against this backdrop, the Bundeswehr established its new Cyber and Information Domain Service on 1 April 2017. Thus, the importance of this new domain is now reflected in our organisational structure.

As the Cyber and Information Domain Service was established, its main tasks were defined. These tasks are considerably more comprehensive than the commonly used shorthand description "cyber" may suggest. The Cyber and Information Domain Service is in charge of protecting and operating the Bundeswehr IT system in Germany and on operations abroad. In addition, the Cyber and Information Domain Service is also responsible for military intelligence and provides situation information in the form of thoroughly evaluated reconnaissance results. We can access enemy IT networks to gather or manipulate information and employ electronic warfare capabilities to ensure the safety of own and friendly units on missions abroad. The Bundeswehr Geoinformation Centre provides each user with individual geo-referenced information – from weather forecasts and soil conditions to digital 3D terrain models.

The Cyber and Information Domain Service has pooled the existing expertise in the Bundeswehr, established and developed additional capabilities and strengthened those areas that will be of particular importance in the future. At the command level, our Joint Cyber and Information Domain Situation Centre provides the Bundeswehr as well as other ministries with a fused situation picture of cyber and information space. As the responsibilities of the Cyber and Information Domain Service increased more and more, the Cyber Operations Centre was established in spring 2018. This agency pools the specific capabilities that are required in today's world to prepare and conduct military cyber operations for the purpose of reconnaissance and effects. As a result, the Bundeswehr possesses an

effective institution whose activities, taken also in cooperation with other actors, will significantly enhance Bundeswehr mission accomplishment in the age of digitalisation and hybrid warfare. This opens additional, non-kinetic courses of action for the military and political leadership and expands the range of suitable responses in crisis situations. The Bundeswehr Cyber Security Centre pools the cyber defence capabilities of the Bundeswehr. It is here that the Bundeswehr computer networks at home and abroad as well as in theatre are monitored 24/7. If cyber attacks are detected or critical IT security incidents occur, Bundeswehr computer emergency response teams restore IT security around the globe.

Cyberspace knows no borders. Hybrid strategies exploit interfaces between responsibilities, for instance internal and external security. Therefore, it is indispensable that we close ranks and share knowledge both at the national level – as part of an interagency approach in cooperation with enterprises, science and society – and at the international level.

Cooperation projects aimed at the mutual exchange of information, knowledge and personnel as well as the mutual opening of basic and advanced training programmes are essential when it comes to strengthening national resilience. In addition, an active exchange at the international level is vital. Attacks from cyberspace as well as campaigns on social media and messenger services do not stop at national borders. Their effects can be felt at the transnational level. International cooperation across national boundaries is absolutely imperative if we are to master these challenges successfully. In the military sector, close bilateral cooperation is already taking place at the EU and NATO level. Here, too, an effective contribution to national security must always be one of our goals.

5G- and Huawei's-Mobile Wireless Network-Technology: Is the UK-Compromise of excluding Huawei from its Core-Network Sufficient?

By Frank Umbach

Dr. Frank Umbach, Research Director at the European Centre for Climate, Energy and Resource Security (EUCERS), King's College, London

This year will decide how fast and secure the newly introduced mobile wireless-network technology of 5G for Europe's industries and critical infrastructures will be deployed and to which extent Europe will become technologically dependent on Huawei and an ever more nationalistic and authoritarian China, which is officially been viewed by the EU as a "systemic rival". Alongside, it will also become clear to which extent the EU member states will accept increasing cybersecurity risks of industrial and political espionage as well as potential sabotage as the result of its wider economic dependencies on China. At the same time, these decisions of the EU member states will also show, to which extent the EU is able to agree on common strategies of its industry, technology and cyber security policy, such as determining and implementing common cyber security standards for 5G networks.

The British government has decided on January 28 that Huawei will be excluded from the core 5G network and restricted to its periphery. It also imposed a future market share cap for Huawei in UK's non-core 5G network from presently 44% to 35% in 2023. Without the British governmental intervention, Huawei would have acquired a future market share of the UK's 5G network up to 70% within the next three years. Within the EU, also other member states – such as Germany – need to decide about Huawei's technology

inclusion by taking into account complex as well as difficult conflicts of objectives and interests. They all need to balance shorter- with longer-term strategic interests of its industry-, technology- and cybersecurity policies as the EU only recommends security guidelines and leaves the technological sovereignty of the 5G-network build-up und Huawei's involvement in the responsibility of the individual member states.

The British Security Council and UK's National Cyber Security Centre (NCSC) have stated that it can manage the remaining risks of deeply entrenched Huawei technologies and shrink them to "acceptable levels" in order to mitigate the key threats of industrial and political espionage, theft or alteration of data, blackmail and network sabotage. But the NCSC has also admitted that the risks of using Huawei's technologies in its 5G network can never be completely removed. Already previously, the NCSC has evaluated Huawei as Britain's only high-risk vendor to build its new ultra-fast high-speed mobile network. The assessment is not only based on China's National Intelligence Law of 2017, which allows the Chinese government to "compel anyone in China to do anything". The NCSC has also warned that China's state and associated actors "have carried out and will continue to carry out cyberattacks against the UK and our interests". It has also repeatedly criticized (as many independent international

cyber security experts for years) that "Huawei's cyber-security and engineering quality is low and its processes opaque". In its 2019 report it confirmed that the Chinese company has also made "no material progress" in addressing "major defects" and significant security concerns already being raised the year before.

Huawei's 5G technology policies are a perfect example of China's long-term thinking by defining the future disruptive technologies and industry applications. As Huawei's technologies are very hardware-centric, they are deliberately not compatible with most of other vendor's technologies. That creates technology path-dependencies over several technology generations. It is another example of China's supply and value chain strategies which seek to control the worldwide research and development, the critical raw materials for the new technologies up to semi-finalized and end products in future key technology sectors.

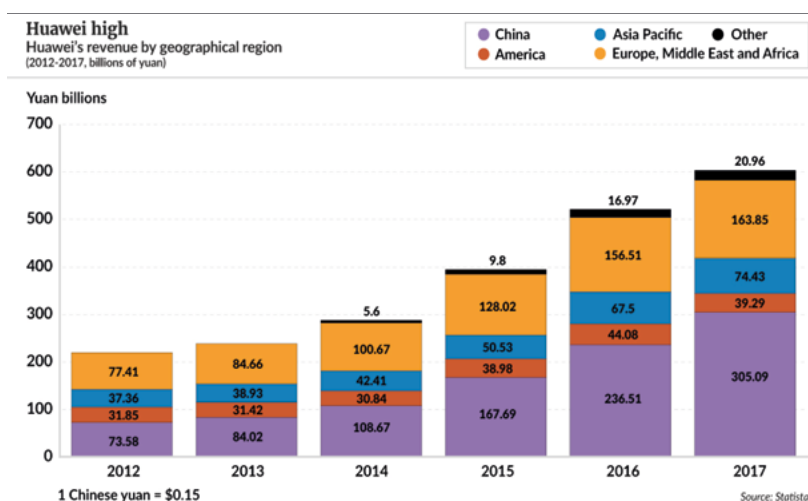## Cyber Security Challenges beyond Huawei

The build-up of national 5G mobile networks might result in a dramatic increase of cyber risks and vulnerabilities as it will connect the future networks of critical infrastructures and "industry 4.0" with millions of unsafe Internet-of-Things-appliances. With every additional connection, it becomes harder to figure out any vulnerabilities of the system. They will also increase

as the traditionally defined "core" (where customer information is stored and processed) of the future 5G-network can't be clearly separated any longer from the periphery (Huawei's antennas and base stations) in contrast to the 3G and 4G networks. More computing power, clouds, servers and processes will move from the core to the periphery as the numerous appliances of the industry 4.0 demand much more decentralized 5G networks.

The future mobile networks will run on advanced software in an increasingly virtualised network that includes the traditional core and the system that manages all the hardware from smartphones to automated factories, driverless cars and telemedicine for rapidly processing data and communication with the network. The various hardware, software application, protocol and code layers include proprietary information, which makes it almost impossible to verify network messages over the hardware back to end consumers such as Huawei (and ultimately China's KP or its secret services).

The dynamic deployment of 5G networks will dramatically change the cybersecurity landscape by increasing the scale of surface attacks and restricting effective surveillance and control. Traditional monitoring methods will become ineffective and obsolete. The 5G network may become so complex that managing the risks of China's involvement could overwhelm all national resources. Therefore, cyber security experts have demanded to disclose the source and programme codes for the 5G networks. But it is contradicting traditional commercial businesses.

Restricting Huawei's technologies to the 5G's periphery alone – as suggested by UK's policies and the EU's recommendations – won't solve many fundamental cybersecurity challenges of the new virtualised networks and, therefore, is not sufficient. Moreover, UK, Germany and few other EU member states may be able to define and implement "acceptable levels" of remaining cybersecurity risks. But 10 other EU member states have neither any institutionalized cybersecurity expertise and capacity nor do they have comparable rigorous security-risk mitigation strategies and any entrenched cybersecurity risk culture to evaluate new cyber risks of new disruptive technologies such as 5G.

Figure 2
Huawei: Revenues by Region 2012 – 2017

Huawei high
Huawei's revenue by geographical region
(2012-2017, billions of yuan)

China | America | Asia Pacific | Europe, Middle East and Africa | Other

www.GISreportsonline.com
Source: FT 2019

Opportunities and Challenges in Developing Military AI Applications

By Yixiang Xu

Yixiang Xu, New Research Initiative Fellow at AICGS working on the Institute's China-Germany-U.S. triangular relationship initiative

Incorporating artificial Intelligence (AI) for national defense is a current priority for countries around the world following its rapid development and multitude of applications in the commercial sector. Increased research and development funding from military research agencies are on course to push the global military AI and cybernetics market to a projected $13.11 billion in 2024 at a compound annual growth rate of 18.66 percent.[1]

Currently, militaries around the world are considering a wide range of AI defense applications. These include intelligence, surveillance and reconnaissance, logistics, cyberspace operations, information operations, command and control, semiautonomous and autonomous vehicles, and lethal autonomous weapon systems (LAWS).[2]

The main benefits of integrating AI into military systems include labor substitution, efficiency, cost reduction, enhancing human capabilities, scaling, and information superiority. AI tools can handle larger volumes of data more efficiently, providing additional analytical capacity for early stage information processing, freeing up human analysts to concentrate on decision-making. AI-enabled tools are especially important in cyberspace operations as they can be trained to perform preemptive and real-time detection, evaluation, and response to network activities on a large scale, thus presenting a more comprehensive and dynamic barrier to attack.[3] AI analysis tools could also help to streamline operations and generate greater cost savings.

In the United States, the Department of Defense launched the Algorithmic Warfare Cross-Functional Team (Project Maven) in 2017 to rapidly incorporate AI into existing DOD systems and is committed to spending $1.75 billion over six years through the Joint Artificial Intelligence Center (JAIC) and $2 billion to invest in dozens of programs through the Defense

1 "Global Military AI and Cybernetics Market to Reach $13.11 Billion by 2024." CISION PR Newswire. November 7, 2019. https://www.prnewswire.com/news-releases/global-military-ai-and-cybernetics-market-to-reach-13-11-billion-by-2024--300953679.html
2 "Artificial Intelligence and National Security, Updated November 2019." Congressional Research Services
3 Scott Rosenberg, "Firewalls Don't Stop Hackers, AI Might," Wired, August 27, 2017. https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/
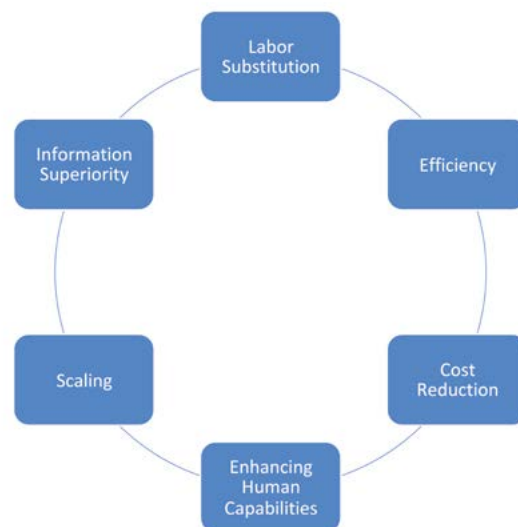
Advanced Research Projects Agency (DARPA).[4] China released a national AI strategy in 2017 that heavily relies on military-civil fusion to facilitate AI technology transfer, which has already yielded results in large-scale visual recognition systems. Russia employs a similar centralized AI development approach and has achieved some early success in developing unmanned ground vehicles. Countries including France, Israel, and South Korea are also expanding efforts to deploy and integrate AI tools in their militaries.

These investments hint at a looming global AI arms race. Unlike the nuclear arms race of the twentieth century, AI-enabled machines will not only perform tasks, but also make decisions. Yet so little of their process and performance impact is understood by those who finance their development or are tasked with their operation. AI algorithms can produce unpredictable results, become subject to bias based on training data, and could experience simultaneous failures. The most sophisticated and highest-performing AI algorithms are often unable to explain their processes. In areas of human-machine interaction, the lack of explanation cautions humans to determine appropriate levels of trust in AI systems.

These concerns about AI become more profound with increasing levels of system autonomy. In the case of LAWS, weapon systems that independently identify and destroy targets without manual human control,

serious ethical and legal questions need to be raised regarding their deployment. The United States has so far refused to participate in negotiating legal or political instruments to regulate autonomous AI weapons at the United Nations. Other countries, while voicing concerns, are unwilling to restrict their own autonomous weapons development. Nevertheless, avoiding the possibility of unpredictable, large-scale, and potentially unaccountable destruction brought by LAWS means we must continue to push for an international, legally binding instrument that ensures meaningful human control over weapons systems.

Some efforts are being made to address potential ethical hazards, although more needs to be done to ensure secure, ethical use of military AI. In the United States, the DOD-commissioned Defense Innovation Board released recommendations on the ethical use of AI by the DOD that are consistent with the Law of War and domestic law, establishing a set of high-level ethics goals.[5] As the development of AI for defense applications moves further along, specific principles should be developed. Amid the increasing public-private partnership in military AI development, governments need to set higher digital infrastructure and cybersecurity standards in the commercial sector, as well as safeguard against exploitation and proliferation with policies including investment screening and export control.

4   "DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies." DARPA, September 7, 2018.
      https://www.darpa.mil/news-events/2018-09-07
5   "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense."
      Defense Innovation Board, October 31, 2019.
      https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF

The U.S. Decoupling Attempt Is Too Costly for the World

By Zhexin Zhang

Dr. Zhexin Zhang, Assistant Research Fellow at the Center for Asia Pacific Studies and Assistant Director of the Institute of Taiwan, Hong Kong, and Macao Studies at the Shanghai Institute for International Studies

Comprehensive and inspiring as it was, the 2019 International Security Forum in Bonn witnessed another step toward the United States decoupling from China, which it accused of "predatory industrial policies," "violating international law and rules," and "threatening values of the free world." This attempt, grounded in accusations that appear unfair, impractical, and harmful to world peace and prosperity, can hardly gain much support from the international community.

It is true that China enjoys significant advantage in global technological, industrial, and commercial competition through its state-led approach (e.g., "Made in China 2025" and the Belt and Road Initiative), and there is much room for China to improve its intellectual property rights protection and ensure an open and fair domestic business environment. Yet, compared with two decades ago, the Chinese market has undeniably become much more open and international rules-based. For instance, China's average tariff rate has dropped from 45 percent to 6.7 percent; the negative list for foreign investment in specific fields has shortened from 190 in 2011 to 40 in 2019, and Presi-

dent Xi Jinping's announcement of five new measures to promote China's opening-up on the second China International Import Expo (CIIE) has further strengthened the confidence of the global business community. Meanwhile, China is making increasing contributions to global governance ranging from tackling climate change and sustainable development to UN peacekeeping and upholding the international system.[1] Considering this progress and the new opportunities China presents to the world, it is senseless to overstate China's imperfectness and feel victimized by China's "growing pains."

Yet, the Trump administration appears keen on decoupling from China by restricting bilateral ties in political, economic, cultural, and other fields. Despite Vice President Mike Pence's statement on 24 October that the United States does not seek to decouple from China, much damage has been done to U.S.-China relations and the U.S. economy as well, including the ongoing trade war that is projected to cost the U.S. economy billions of dollars and 300,000 jobs[2]; technological sanctions against Chinese companies that have much

1   White Paper on "China and the World in the New Era," September 27, 2019.
2   CBS, September 12, 2019.

disrupted global industrial chains; increasing limitations to people-to-people exchange that have reduced Chinese visitors to the United States by 20 percent; growing regional tension over Taiwan, Hong Kong, and the South China Sea due to U.S. intervention; and, as this Bonn Forum showcases, a global public opinion campaign to alienate China from all "like-minded countries." As a result, the Trump administration has begun to encounter a backlash both at home (e.g., some members of Congress have proposed legislation to curb presidential tariff power) and, ironically, from the 192 American enterprises that attended the second CIIE, an 18 percent increase from last year, in spite of the administration's decoupling advocacy. Opposition has also emerged from abroad (e.g., the UK and Germany seem to hold an open stance to China's Huawei participating in their 5G network construction); as close partners of the Indo-Pacific Strategy, both India and Japan have openly rejected the scenario of building a geopolitical bloc against China, but rather seek to bring relations with China to "new heights" instead. With the presidential election approaching, the United States' decoupling goals will be even more difficult to achieve.

That said, if the Trump and later U.S. administrations are determined to further decouple from China, the world will certainly face a gloomy future: the IMF predicts that the lasting trade war will cost the global economy $700 billion by 2020, slowing global economic growth to lower than 3 percent and triggering more protectionist and unilateral policies in many countries; as more trade and technological barriers emerge, global investors will have less incentive to invest, further exacerbating unemployment and radical populism in developing and developed countries alike. China's close economic partners, including EU countries, will be compelled to take sides between China and the United States. Worst of all, a new Cold War may take shape where an isolated and cornered China becomes more politically and economically closed and seeks to expand its sphere of security and economic influence worldwide, which, like the Cold War decades ago, truly reflects the much-hyped notion of today – "one world, two systems."

Fortunately, this is not a reality yet. As Mao Zedong (and similarly, Carl Schmitt) famously put it, politics is an art to "foster as many comrades (friends) and as few enemies as possible." Indeed, after three decades of globalization, the interdependent world cannot afford deliberate schisms and manufactured enemies, but rather needs more common understanding and consultation on the shared interests and coordinated approaches among countries, which I hope can become the dominant theme for this Forum next year.

Co-Host:

American Institute for Contemporary German Studies
JOHNS HOPKINS UNIVERSITY

A very special thanks also to Guido Goldman.

Special Partner:

KONRAD ADENAUER STIFTUNG

Partners:

U.S. Consulate General
Düsseldorf

DGAP
Advancing foreign policy. Since 1955.

STADT.
CITY.
VILLE.
BONN.

CYBER
SECURITY
CLUSTER BONN

Center for Advanced Security,
Strategic and Integration Studies (CASSIS)
University of Bonn
Römerstraße 164
53117 Bonn, Germany
cassis.uni-bonn.de