ISSN 1812-1098, e-ISSN 1812-2973

# CONNECTIONS

## THE QUARTERLY JOURNAL

Vol. 15, no. 2, Spring 2016

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

http://dx.doi.org/10.11610/Connections.15.2

## Contents

# Vol. 15, no. 2, Spring 2016

## Editorial

Emerging Security Challenges: An Introduction 5
*Detlef Puhl*

## Research Articles

Policy and the Internet of Things 9
*Sean S. Costigan and Gustav Lindstrom*

Industry and Policy: Partnerships in Disruptive Times 19
*Leendert van Bochoven*

Nanotechnology and Global Security 31
*Adrian M. Ionescu*

Biology's Misuse Potential 48
*Filippa Lentzos*

Hybrid Warfare and the Changing Character of Conflict 65
*Bastian Giegerich*

Making Sense of Hybrid Warfare 73
*James K. Wither*

Non-State Actors in the Russo-Ukrainian War 89
*Joshua P. Mulford*

Cyber Operations and Gray Zones: Challenges for NATO 109
*Oliver Fitton*

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Detlef Puhl, *Connections QJ* 15, no. 2 (2016): 5-7
http://dx.doi.org/10.11610/Connections.15.2.00

**Editorial**

# Emerging Security Challenges: An Introduction

*Detlef Puhl*

*Emerging Security Challenges Division, NATO International Staff*

The security landscape at the beginning of the 21st century is a fluid and dynamic one, characterized by developments in technology, in weapons and communications systems as well as by shifts in the international political landscape and organizational structures of non-state actors posing serious and imminent threats to national and international security. Within this environment NATO finds itself at a crossroads. Its Strategic Concept, adopted in Lisbon in November 2010, marks the beginning of its adjustment to this new reality, reflecting a security environment with effects far beyond NATO and its partners – an environment which will see the fundamental global shifts continue in the coming years: In the global distribution of power, including revisionist activities in our immediate neighborhood and a fundamental challenge to our rules-based international order by mainly radical islamist organizations; in demographics; in economics; in technology; in the environment. Faced by such very different global challenges to our security, NATO must seek to maintain its cohesion and develop a broader notion of transatlantic security and enhance its relevance in meeting modern day threats and challenges.

In the face of many non-traditional, mostly non-military security challenges, which affect Allies in different ways, the Alliance needs to reaffirm and enhance its cohesion both within the organization and with its Partners and beyond. It needs to develop policies and activities if they don’t want to be overwhelmed by those new challenges. In order to fulfill this task, Allies need new and more expertise about those challenges, within the organization and shared by all Allies and Partners. They need to raise and maintain awareness of them and actively cooperate more with outside actors. In this regard, neutral and non-aligned nations and their seasoned experience in the exercise of soft power have much to offer.

To this end, the Partnership for Peace Consortium has created its Emerging Security Challenges Working Group to promote reflection on a number of very fundamental questions:

- What exactly are "Emerging Security Challenges" which NATO deals with in a specific division of its International Staff, created in 2010?
- What role is there to play for the military in addressing them?
- How do we need to be organized to meet those challenges?
- What can the Alliance and its Partners, in cooperation with neutral and non-aligned nations and others, do to help guide this process?
- What impact does addressing these challenges collectively have on the way in which we interact internationally?
- How do we need to educate and train our staff and leaders so they are able to cooperate intelligently in an ever more complex and interconnected security environment?

In effect, we need to think, talk, discuss collectively about an emerging security environment which is very different from what we are used to. This is true for all of our countries, for the Alliance as an organization, and for the whole international community. This environment will keep changing in sometimes surprising and unexpected ways and we don't know what comes next. It will be critical for Allies and their Partners to find compatible, if not similar or even common answers to these challenges. Some consider NATO to be a useful and proven framework and tool to commonly address such challenges to our security; others prefer to rely on national capabilities and bilateral cooperation, charging NATO with providing the indispensable back-up to territorial security.

The Emerging Security Challenges Working Group has discussed many of these questions in the six workshops it has held so far. Its ambition is to examine and raise awareness of emerging technologies and their impact on security policy. It also strives to foster engagement between NATO nations and Partner nations – offering a platform for discussions among NATO and partner experts. It finally seeks to develop curricula for education of military and civilian leadership who have to deal with these complex issues.

This special edition of "Connections" presents an overview of some of the topics which the Working Group considers to constitute "emerging security challenges." This list can and will be completed over time, as technological innovation and political developments in the international community continue to evolve.

The authors of the first five papers in this edition have all presented their thoughts on the issue to the Emerging Security Challenges Working Group and spurred interesting discussions in different workshops, which resulted in a number of Policy Papers and Background Papers published by the PfP Consortium. Here, they all address the question of why policy makers in the security field should care about the particular issue, what are fundamental technological trends, and potential security implications to policy making in our nations and within NATO. Authors from outside the Working Group complement these reflections, focusing on particular issues of what is now called "hybrid warfare" in the context of the Russian-Ukrainian conflict.

The Co-Chairs thank all the authors and contributors to what will continue to constitute a relevant and fascinating debate on international security policy.

## About the author

Since 2011, Dr. Detlef Puhl serves as Senior Advisor for Strategic Communication to the Assistant Secretary General of NATO for Emerging Security Challenges, delegated from the German Ministry of Defense. Previously, from 2008 to 2011, he was Assistant Director at the "Délégation aux Affaires Stratégiques," the Policy Planning Staff of the French Ministry of Defense. Prior to that, from 2002 to 2008, as Associate Dean of the "College for International and Security Studies" at the George C. Marshall Center in Garmisch-Partenkirchen, he worked very closely with the US Department of Defense and US European Command, as well as representatives from Central and Eastern Europe and Eurasia. From 1998 to 2001, he was Director of Press and Information and Spokesman of the German Ministry of Defense. Until then, Dr. Puhl had worked for many years as military and security policy correspondent of the "Stuttgarter Zeitung" in Bonn and Stuttgart.
E-mail: detlef.puhl@gmx.net

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Sean Costigan and Gustav Lindstrom,
*Connections QJ* 15, no. 2 (2016): 9-18
http://dx.doi.org/10.11610/Connections.15.2.01

**Research Article**

# Policy and the Internet of Things

*Sean S. Costigan* [a] *and Gustav Lindstrom* [b]

[a] *The New School (link is external), New York, NY, http://www.newschool.edu/*

[b] *Geneva Centre for Security Policy, http://www.gcsp.ch/*

**Abstract**: Cybersecurity has steadily crept to the top of the national security agenda. Simultaneously, a merger of the physical and virtual worlds is noticeably underway. A confluence of technologies has come together to make this possible under the rubric known as the Internet of Things (IoT). This merger will bring sensors and computing devices totaling in the billions to connect objects together in a network that does not require human intervention, along with which will come much vaunted benefits, knowable risks, uncertainties and considerable security dilemmas. Using the past as a predictor of future behavior, a vast increase in hackable devices will create equally vast vulnerabilities that will now touch the physical world. Yet the IoT will also present opportunities that are just now being imagined, likely making the Internet revolution seem small by comparison. While technological growth often appears to outpace policy, government retains the power to convene and ultimately to regulate. This article examines why policymakers should care about the IoT, the significant trends for the next five to ten years, and likely security implications stemming from those trends. The article finalizes with an overview of policy considerations.

**Keywords**: Internet of Things, Industrial Internet, security implications of IoT, machine communications, critical infrastructures.

## Introduction

Over the past decade, cybersecurity concerns have steadily crept to the top of national and international security agendas. However, with the focus mainly on policies and strategy, rapid technological developments continue to undermine policymakers' understanding of cyber risks and opportunities. One such development is the Internet of Things (IoT).

While the Internet of Things is not widely discussed among policy circles, it is nonetheless likely to substantially impact how individuals, institutions and societies interact in the future. In brief, the IoT refers to the interconnection of uniquely identifiable, machine-to-machine devices with the Internet. A relatively well-known example from retail industry is the use of radio frequency identification devices (RFID) to track the location of goods and inventory.

According to one estimate, there are currently about 9 billion devices connected to the Internet. This number—which is already greater than the global population—is expected to grow dramatically over the next ten years. According to recent calculations, every second 127 new devices are being added to the Internet.[1] Other projections from notable institutions suggest roughly 50 billion to 1 trillion devices will be connected to the Internet by around 2025, impacting how business is carried out in fields ranging from health care to security policy.  This is currently yielding  new visions  such as the movement to-

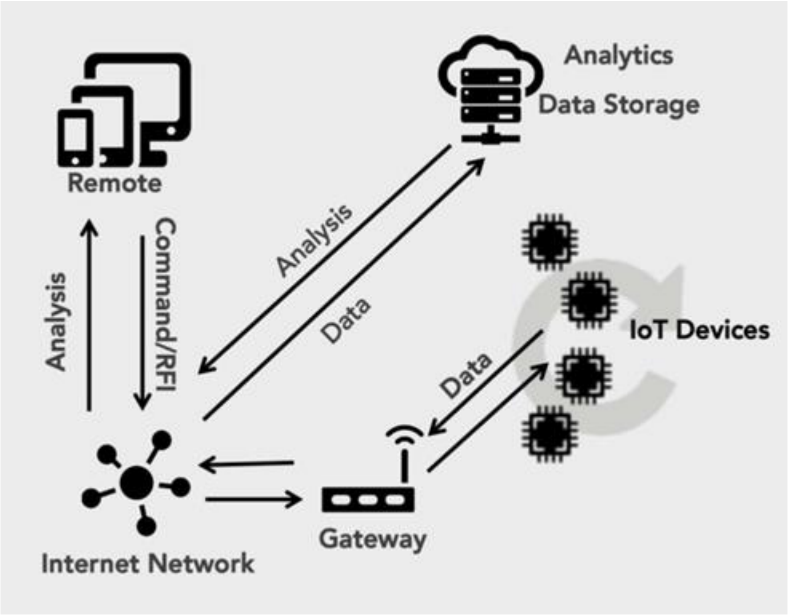


**Figure 1: The IoT Ecosystem (Source: Business Insider, www.businessinsider.com).**

[1] "127 devices added to the Internet each second, but Congress is clueless about IoT," *NetworkWorld*, 1 July 2015, available at http://www.networkworld.com/article/2942596/microsoft-subnet/127-devices-added-to-the-internet-each-second-but-congress-is-clueless-about-iot.html.

wards as the “Internet of Everything” (Cisco) or the “Industrial Internet” (General Electric). General Electric estimates that the “Industrial Internet” will add $10 to $15 trillion to the global GDP within the next 20 years. With growth of that scale, the IoT is set to usher in a new era of ubiquitous computing that will make the changes brought about by the Internet look small by comparison.

This article examines why policymakers should care about IoT, the significant trends for the next five to ten years, and possible security implications stemming from those trends. The article finalizes with an overview of policy considerations.

## Why the Internet of Things Matters

We suggest that there are three main reasons why policymakers should care about the IoT. First, the Internet of Things has the potential to contribute to substantial economic growth. Current developments, such as the gradual introduction of smart meters (for energy efficiency) and driverless vehicles (for transport and logistics) represent just a small sample of the opportunities offered by IoT. Applications are possible in most fields, opening the door to economic growth primarily via efficiency gains and new services that need not entail human intervention. A 2015 study by Accenture suggests IoT can add $10.6 trillion to the cumulative GDP of 20 developed and emerging economies that represent over 75% of the world’s economic output.[2] Another report by the McKinsey Global Institute estimates an IoT economic impact of $2.7 to $6.2 trillion annually by 2025.[3]

Second, the IoT will impact diverse and multiple fields, enabling advances and efficiencies across disciplines as opposed to within one or two areas. With this in mind, the areas that are most likely to gain from the IoT are health care, infrastructure, and public sector services.[4] Given current trends, the applications enabled by the IoT will be wide ranging and some cases only limited by imagination. Prospects range from “smart cities” to “personalized healthcare.” Specific examples might include a more efficient traffic flow as street signs or stop lights that can communicate with each other and with vehicles in their

[2] Mark Purdy and Ladan Davarzani, “The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity” (Accenture Strategy, 2015), available at https://www.accenture.com/_acnmedia/Accenture/ Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_18/Accenture-Industrial-Internet-Things-Growth-Game-Changer.pdf.

[3] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, “Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy,” Report (McKinsey Global Institute, May 2013), available at http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies.

[4] For additional information on the economic impact of the IoT see Charles Saidu, Adamu Usman, and Peter Ogedebe, “Internet of Things: Impact on Economy,” *British Journal of Mathematics & Computer Science* 7:4 (2015): 241–251.

proximity. IoT sensors can be placed on infrastructures such as bridges to identify micro fissures and cracks, enabling preventative efforts to prolong their lifespan. Within the defense sector, IoT may be used to enhance logistics and transport. IoT may also play a role in autonomous weapons systems, especially as consideration is given to automated systems.

Third, policymakers should care about IoT because there are probable drawbacks and unintended consequences, some of which can have implications for society, critical services and infrastructures. At the minimum, societal dependency on the IoT and a growing "attack surface" will have significant and hard to predict consequences. These issues will be examined in greater depth in the section on potential security implications.

## Future IoT trends

Looking ahead, three interrelated trends stand out vis-a-vis the IoT. The first is an accelerating rate of diffusion which, though in its infancy, is already visible today. To illustrate, there was a 30% increase in things connected to the Internet from 2014 to 2015. Table 1 below provides an illustration of projections across different sectors.

**Table 1. IoT Diffusion by Sector in Billions of Devices (2015–2020).**

| Category | 2015 | 2020 | Percent Increase |
|---|---|---|---|
| **Automotive** | 372 | 3511 | 944 % |
| **Consumer** | 2,875 | 13,173 | 458 % |
| **Generic business** | 624 | 5,159 | 827 % |
| **Vertical business** | 1,009 | 3,164 | 314 % |
| **Total** | **4,880** | **25,007** | **512 %** |

Source: Gartner, "4.9 Billion Connected 'Things' will be in use in 2015, November 2014.

As shown in the table, the total percentage increase across the four categories examined is approximately 500%, with most growth in IoT diffusion expected in the automotive sector. If these trajectories are even close to accurate, society will be facing substantial changes in how it collects, monitors, and processes information. This trend will be fuelled by two other distinct developments: 1) Continued developments in communications protocols (including wireless), energy storage (e.g. for batteries), microelectromechanical systems (MEMS), and computing power, and 2) Developments in areas that can impact the applicability of IoT such as nanotechnology, artificial intelligence, and data

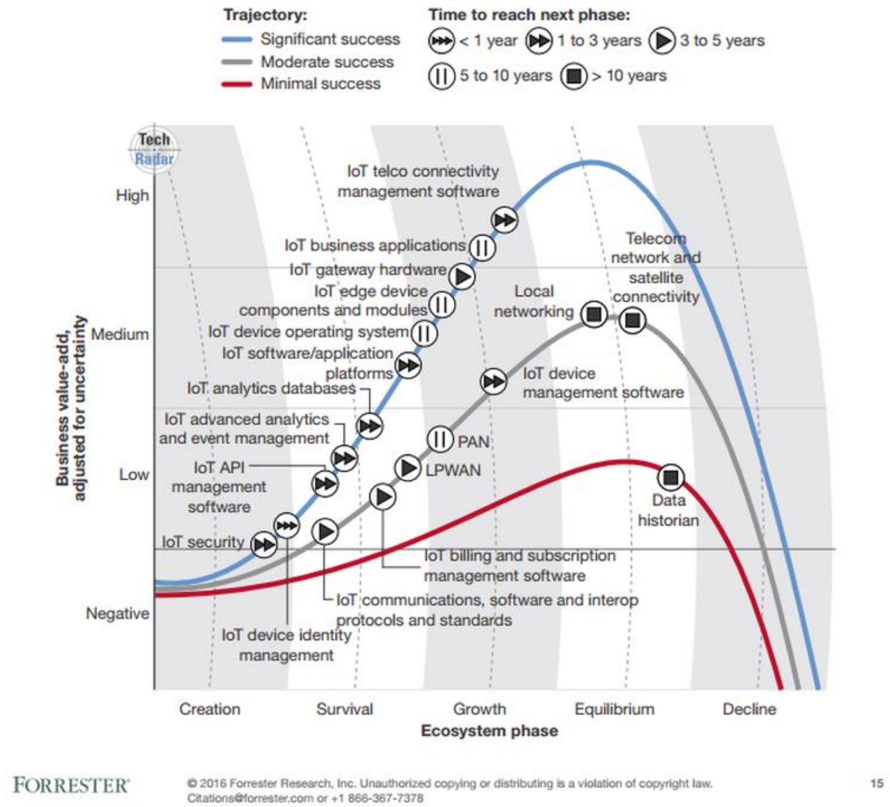


**Figure 2: IOT Business Value-Add Over 10 Years**

Source: Forrester Research, www.zdnet.com/article/internet-of-things-security-years-away-from-being-fully-baked-says-forrester.

science.[5] Combined, these two will enhance both the reach and applicability of IoT across a variety of sectors.

A second trend is the rapid growth in machine (M2M) communications. As IoT diffusion increases, so will the direct communication between devices that are connected to the Internet, either through wired or wireless form. One estimate forecasts the total number of M2M connection worldwide to increase from roughly 196 million to 361 million in 2018 – an increase of 184% over three years.[6] This trend is significant since we cannot fully predict the consequences stemming from the growth in M2M. In a world were communications

[5] For reference, there are multiple protocols that facilitate communication across devices. These range from wireless protocols such as ZigBee, Bluetooth, and BACnet to developing standards such as RPL, CoAP, and 6LoWPAN.

[6] The Statistics Portal, Statista, 2016. Available at www.statista.com/statistics/295635/total-number-m2m-connections-worldwide.

are between an individual and a device, or between two devices, the outcomes are easier to predict. In an IoT world, data and communications will become ubiquitous.

For example, if a sensor is tasked to monitor the temperature in a location and is programmed to send a warning to an individual or other device when the temperature reaches a certain point, the directionality is clear and simple. With devices increasingly communicating instantaneously while managing or monitoring processes, the relationship becomes multidimensional, complex and possibly more stochastic or random. Given this trend, the ability to control specific relationships between devices may become more complex and unpredictable.

Lastly, growth in IoT and M2M will deliver ever larger amounts of machine-generated data. According to a 2012 IDC Digital Universe study, machine generated data is projected to increase by a factor of 15 by 2020.[7] IDC further notes that about 40% of all data is likely to be machine generated by 2020. This trend will have implications across various areas, specifically on how the data is gathered, processed, stored, and shared. Here, too, policy lags behind.

## Potential Security Implications

Two key security implications are likely to arise from the IoT revolution. The first and foremost is addressing the lack of security functions in the majority of sensors and actuators that make up the backbone of the IoT. Specifically, as companies push out more minimally viable products in a rush to meet demand, low-cost sensors and actuators for data collection, monitoring, and process optimization will remain unlikely to have properly embedded security functions within them. Security is apt to remain an expensive afterthought.

Moreover, sensors tend to suffer from limited memory capability and computational power, further diminishing opportunities to produce IoT devices with appropriate security protocols (which frequently is not a primordial goal in the mind of developers). This inherent weakness in IoT translates into possible societal vulnerabilities as devices across sectors ranging from health to agriculture can be compromised.

This IoT vulnerability is already associated with critical infrastructure protection, where there is concern that industrial control systems such as Supervisory Control And Data Acquisition (SCADA) may be compromised in a way that blocks a critical service or infrastructure. With billions of new devices being brought online, the attack surface of modern society will vastly increase, bringing with it the same ever-present vulnerabilities that we see today but at a greater scale. Cascading problems may be more likely, as systems will control other systems. Control systems, which previously were principally accessed via

[7] John Gantz and David Reinsel, "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East" (IDC, December 2012), available at www.emc.com/leadership/digital-universe/2012iview/index.htm.

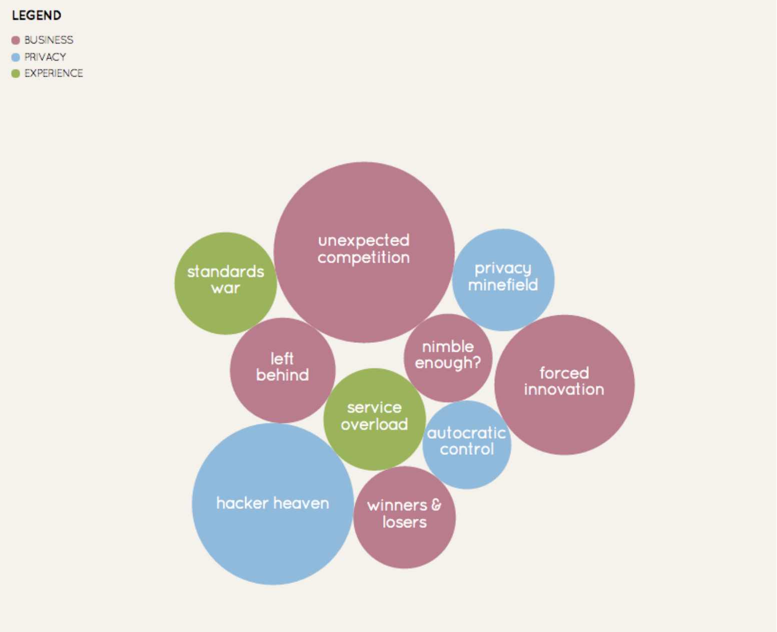


**Figure 3: Challenges for the IoT.**
Source: Information is Beautiful, http://www.informationisbeautiful.net.

proprietary systems that were not connected to the Internet, are now increasingly accessible through commercial-off the shelf programs that can be accessed online. This vulnerability has gained increased attention after specific attacks on Iran's nuclear centrifuges (via Stuxnet) and Saudi Aramco's workstations (via Shamoon). In short, the IoT is apt to make the Internet even less secure for everyone.

A second challenge posed by IoT is the balance between individual privacy rights and security requirements. As Bruce Schneier recently put it, "surveillance is the business model of the Internet"[8] and that is set to vastly increase in an IoT world. The impact is likely to be underestimated in the short- to medium-term, especially as IoT is combined with developments in other fields. For example, the placement of sensors in clothing materials—facilitated by advances in nanotechnology—opens the door to monitoring information on an individuals' location and possibly some vital signs. Looking ahead, should the use of implanted sensors for monitoring health status become more accepted, it could result in the collection of large-scale data on individuals' health status.

[8] Bruce Schneier, "The Internet of Things Talks About You Behind Your Back," 13 January 2016, available at https://www.schneier.com/blog/archives/2016/01/the_internet_of.html.

This development is already underway with the so-called wearables movement, but once again will be likely to vastly increase in power and diffusion in the next decade. While there could be many benefits from a more personalized health care system, it may also raise challenges with respect to individuals' access to health insurance packages and ability to secure employment opportunities.

The already complex question of balancing privacy and security rights will thus become increasingly thorny. With the prospect of billions of sensors and IoT devices deployed, policymakers will have to more carefully analyze the ways in which data can be compromised. Thus, beyond collection issues, a greater understanding of vulnerabilities at other stages will be needed; for example: how IoT information is collected and used (for example is it shared with third parties?); whether there are risks that sensitive IoT data be accessed by third parties; and how the value of data changes when it is combined with other data.[9]

## Policy Considerations

The movement towards the Internet of Things presents several substantive policy considerations for policymakers. The paramount issue is how to best position national policies and strategies to take advantage of IoT benefits while minimizing possible risks associated with more devices connected to the Internet. Precious few countries (such as the Czech Republic, United Kingdom and Australia) and organizations have done such an analysis at the national level, with other countries either adopting a watch and wait approach or none at all.

Second, policymakers should be aware of the chokepoints that might negatively affect the opportunities presented by IoT. Currently, there are a number of outstanding issues that will impact the way IoT evolves, ranging from technical considerations—such as the ability to agree on specific standards for IoT network communication—to strategic considerations regarding the applicability of IoT within the security realm.

Third, policymakers should try to better understand the unintended consequences stemming from the IoT revolution. For example, how might employment and national economies be disrupted as certain skill sets become redundant? From a legal angle, how might the IoT impact laws or regulation safeguards? From a technical perspective, what are implications on divergent views concerning how IoT devices are configured and managed (e.g. should devices announce themselves? How should they be authenticated? Should the IP-addresses for IoT devices be generated automatically or should they be auto generated)? Needless to say, decisions concerning technical arrangements can result in multiple unintended consequences across sectors.

[9] Rolf Weber, "Internet of Things: Privacy Issues Revisited", *Computer Law & Security Review* 31 (2015): 618–627.

Fourth, government should encourage active discussions on embedding security in products. It is increasingly clear that there are limited incentives for IoT device makers to integrate security protocols into their products. On the other hand, it is likewise becoming evident that a lacking or weak security profile may result in dire consequences. Recent examples include the demonstrated ability to gain access to an aircrafts' velocity and steering functions via the on-board entertainment system,[10] successful attempts to hack IoT enabled medical devices such as insulin pumps,[11] search engines that allow people to peer on unsecured baby cameras,[12] and weaknesses in automobiles and other driverless vehicles.[13] As these vulnerabilities are better known and mapped, the more difficult it will be for industry and policy circles to leave them unattended.

Finally, government retains the power to convene and ultimately to regulate. As such, government has responsibility to stay ahead of the curve on security concerns and has the power to encourage the adoption of new technologies and standards that should produce considerable gains for society. As a starting point to ameliorate the security situation and to improve the adoption of more secure devices, government should fund expert-level research that could be used to initiate a consistent "systems approach" to security and the IoT. Such an approach is apt to pay dividends for decades to come.

[10] Dylan Tweney, "FBI Says This Hacker Took Over a Plane through Its In-flight Entertainment System," *VentureBeat*, 17 May 2015, available at venturebeat.com/2015/05/17/fbi-says-this-hacker-took-over-a-plane-through-its-in-flight-entertainment-system/.

[11] Eric Basu, "Hacking Insulin Pumps and Other Medical Devices," *Forbes*, 13 August 2013, available at www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#2715e4857a0b5822f59f4327.

[12] J.M. Porup, "How to Search the Internet of Things for Photos of Sleeping Babies," *ArsTechnica*, 19 January 2016, available at http://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[13] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It," *Wired*, 21 July 2015, available at http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

## About the authors

**Sean S. Costigan** is a consultant and analyst on technology, risk and security. He is Senior Advisor for Emerging Security Challenges at the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes and Lecturer at The New School, in New York City. He leads a joint NATO/PfPC cybersecurity curriculum development effort for European defense academies. He was recently a member of the Intelligence Community Analyst Private Sector Program for the U.S. Department of Homeland Security and ODNI, and has consulted for the U.S. federal government on information technology, cybersecurity, environmental security and foresight. His latest book *Cyberspaces and Global Affairs* is available in English and Chinese.
E-mail: costigs@newschool.edu

**Gustav Lindstrom** is the head of the Emerging Security Challenges Program at the Geneva Centre for Security Policy (GCSP). Previously, he headed the GCSP's Euro-Atlantic Security Program and was the Director of the European Training Course. He currently represents the GCSP on the Executive Academic Board of the European Security and Defence College and serves as the co-chair of the PfP-C Emerging Security Challenges Working Group. Dr. Lindstrom received his doctorate in Policy Analysis from the RAND Graduate School and M.A. in International Policy Studies from Stanford University. Prior to his tenure at the GCSP, Dr. Lindstrom served as a Senior Research Fellow at the EU Institute for Security Studies (EUISS). His areas of interest and expertise include European Common Security and Defence Policy (CSDP), emerging security challenges, non-proliferation & disarmament, and cyber security.
E-mail: g.lindstrom@gcsp.ch.

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

L. van Bochoven, *Connections QJ* 15, no. 2 (2016): 19-29
http://dx.doi.org/10.11610/Connections.15.2.02

**Research Article**

# Industry and Policy: Partnerships in Disruptive Times

*Leendert van Bochoven*

*IBM Industry Academy, http://www-935.ibm.com/industries/industryacademy/*

**Abstract**: The rate of (technological) change in today´s dynamic environment calls for new policies and collaboration models between governments and industry. Two key elements will underpin successful policies for dealing with innovation and the impact of technology: an innovation ecosystem and an innovation platform. Just like companies are involving customers in private sector innovation, governments are seeking to involve citizens. There is a growing trend to engage citizens more and more in the co-creation of public services. The citizen co-creation approach also has merits for the defense and security industry, and there are several successful examples showcasing new ways of collaboration, overcoming the traditional obstacles.

Three key recommendations will enable governments to overcome innovation challenges. These recommendations depend on two essential enablers to deal with disruptive innovation in government organizations: an innovation ecosystem and an innovation platform. Without both, innovation is for sure going to fail. Given the rate of unprecedented technological change, governments, militaries and businesses have to find creative ways to work and innovate together.

**Keywords**: Policy, industry, technology, innovation, ecosystem, cognitive, public-private collaboration, partnerships, co-creation.

The world is going through a number of unprecedented changes, including in geopolitics, technology, and the climate. This dynamic environment calls for new forms of collaboration between government and industry, as the traditional arm's-length client-provider relationship is not responsive enough for today's rapid pace of change. The existing collaboration models are running out of steam. Where in the past government collaboration was limited to small coalitions of like-minded partners, for today and tomorrow there must be a change in collaboration models beyond the typical approach. These new collaboration models require different policies to be workable in the government space. This article will explore key elements of these policies. Most are not new and have been called for many times, but the urgency to implement them keeps increasing due to the changes in the world. Two key elements will underpin successful policies for dealing with innovation and the impact of technology: an innovation ecosystem and an innovation platform.

## Making the Case for Change

Many reports describe an emerging picture of a mind-boggling number of devices and sensors connected to the Internet. For example, Gartner predicts that by 2020, 35 billion objects will be online. Already in 2016, the spending on new Internet of Things (IoT) hardware will exceed $2.5 million per minute.[1] The digital and physical world will continue to integrate and become increasingly interconnected. Physical things will have a digital layer around them, and each of these things will have a digital footprint and thus generate an incredible volume of data. Not only will the volume of data increase, but the nature of the data will change as well. This is disrupting existing approaches to computing while opening vast new opportunities to create value.

That is especially true of “edge data,” which includes all the new forms of data generated by users and their devices, such as tablets, smartphones, sensors and more. It is fast-paced, dynamic, unstructured, temporal in nature, unlike any prior data creation model. Edge data is incredibly rich in offering an understanding of context and, therefore, has potentially very high value. This is but one example of a technology trend that already has a big impact on organizations, and there is rather a confluence of developments. Each of the trends in nano, bio and information technology will have its own line of development. Information technology alone will have a disruptive effect, and certainly when it is combined with new possibilities in nano and bio technology.

## Partnership Models in the Age of Disruptive Innovation

Management guru Clayton Christensen coined the term “disruptive technologies” in his book, “The Innovators Dilemma,” in 1997.[2] This was later followed by the term “disruptive innovation” to describe how new entrants target the bottom of a market and then relentlessly move up market, eventually ousting established providers. However, what was once a relatively rare phenomenon

[1] Gartner, “Forecast: Internet of Things, Endpoints and Associated Services, Worldwide,” 29 October 2015, available at https://www.gartner.com/doc/3159717/forecast-internet-things--endpoints.

[2] Clayton Christensen, *The Innovators Dilemma: When New Technologies Cause Great Firms to Fail* (Boston, MA: Harvard Business Review Press, 1997).

has now become a regular occurrence. Innovations that harness new technologies or business models, or exploit old technologies in new ways, are emerging on an almost daily basis. Disruptive is not a popular word in government circles, but the accelerating digitization and impact of radical technology changes are certainly also disrupting government.

In 2012, IBM's Institute for Business Value (IBV) conducted its fifth biennial "Global CEO Study."[3] This was based on more than 1700 interviews with CEOs from 64 countries across 18 industries, including government. As part of the analysis, the IBV sought to understand differences between responses of CEOs in outperforming organizations and those in underperforming organizations. According to the study, of all the external forces that could impact their organizations over the next three to five years, CEOs see change in technology as the most critical, as technological factors are by far the biggest of the various external forces buffeting their organizations. Technology was at the top of the list back in 2012, and the view is no different in the 2015 CEO study.[4] For governments, the impact of budgets topped the list (89% of the government leaders cited this as the most important factor) and technological factors (78%) as the second external factor influencing government organizations.

Meanwhile, the 2015 CEO study, "Redefining Boundaries," examines how businesses are responding to these new disruptive innovations. A few years ago, business leaders could see the competition coming. The biggest risk was the advent of a new rival with a better or cheaper product or service. The threat could be offset by improving or expanding the range of products and services on offer, or getting to market more efficiently and imaginatively. Nowadays companies ask themselves if they are about to be "Ubered." While most government organizations are not faced with these competitive challenges, there are both implications for governments and lessons to be learned from how market leaders are coping with these innovation challenges. There are two major implications and takeaways for government leaders. Firstly, the strategies and tactics that will enable private sector organizations to effectively compete amidst the disruption of industry convergence can also enable government organizations to become more agile, effective and efficient while also improving innovation capacity. Government organizations can draw on lessons from the private sector to help transform business and operating models. Secondly, governments and key actors in the public sector (e.g. educational institutions, economic development and investment promotion organizations) must create business environments that enable private sector companies to thrive

[3] IBM Institute for Business Value, *Leading Through Connections: Insights from the Global Chief Executive Officer Study* (IBM, 2012), available at http://www-935.ibm.com/services/multimedia/anz_ceo_study_2012.pdf.

[4] IBM Institute for Business Value, *Redefining Boundaries: The Global C-suite Study* (IBM, 2015), available at www-935.ibm.com/services/c-suite/study/pdf/ibm_global_csuite_study-2015.pdf.

amidst this disruption to ensure economic vitality and sustainable economic growth in regional economies.

While both takeaways apply to government in general, they equally apply to the defense and security sector. Defense and intelligence organizations must collaborate much more closely with industry in order to tackle disruptive technologies and innovate the "business of security," especially because their adversaries also have access to most of these technologies, without the burden of lengthy acquisition processes. State and non-state actors apply and exploit innovative technologies in order to disrupt the security environment and challenge the status quo. For example, just a few years ago cyber security concerns were just blips on the radar screen. Today, the majority of business, government and military leaders, irrespective of role or the technology they selected, think cyber security is a top risk.

## Amplifying Innovation with Partnerships

The changing landscape has led to the question of what government organizations are doing to deal with external forces and how they ensure they outperform their peers. The 2012 IBV study concluded that one the three imperatives essential for outperformance is "amplifying innovation with partnerships."[5] This was further reflected in the survey, as nearly 70 percent of CEOs responded that they are aiming to pursue extensive partnerships.

Rising complexity and escalating competition have made partnering a core innovation strategy for many organizations, but to enable sustained, fruitful innovation partnerships, organizations will need deeper, more integrated relationships. Partner organizations will have to share collaborative environments, data and control. They will need to enable close working relationships among staff, and not just executives. Even when an organization is performing well, CEOs must occasionally break from the status quo and introduce new external catalysts, unexpected partners and some intentionally disruptive thinking. The same holds true for government organizations.

The aforementioned study reveals three new ways in which organizations can connect with partners to accelerate innovation.[6] The first is to fundamentally change how to partner. As the pressure to innovate mounts, organizations are reevaluating how they engage partners. This is also necessary because of the increasing costs to innovate. These costs are not always visible in an organization, but certainly have to be taken into account when discussing new approaches to partnering. They are often also overlooked in partnerships between the government and private sector and can become a real stumbling block for sustainable partnering models.

Partnership models can achieve differentiation through social innovation by extending communication and collaboration tools. Peers can interact within

[5] IBM Institute for Business Value, *Leading Through Connections*, page 43 onwards.

[6] Ibid., 48–50

and across organizations, allowing for integration of data resources to reveal unexpected, mutually beneficial insights. The boundaries between organizations are becoming more porous, while interactions span more functions and are more continuous. A good example in the NATO context is the Innovation Hub of NATO's Allied Command Transformation, which enables collaboration among a wide range of partners. Another way to change the partnership model is to expand the scope of the partnerships. Organizations should evaluate ways to extend and connect existing partnerships on innovation to include ideation, research and development and sales, marketing or human resources. The partnership model must also address the governance challenge. This may prove to be the most difficult to tackle, especially in partnership models between the government and private sector. The partnership model should establish ways to share key aspects of control, such as prioritization, decision-making and funding, that are traditionally dominated by one partner. As the costs to innovate increase, the need for transparency is also rising. Control and governance must increasingly be shared.

A second way organizations can connect with partners to accelerate innovation is to make partnerships personal.[7] Technology now presents opportunities for much deeper connections with partners, while this interconnectedness allows for more opportunities for innovation – both spontaneous and orchestrated. To this end, the responsibility for managing partnerships can be broadened within the organization, as it is not just the responsibility of a single unit in the organization. This means that the capability for relationship management must be embedded across the organization and use centralized alliance management functions to supply specialized skills. In US military terms: partnerships are not just the responsibility of the senior officer in charge of Civil-Military Co-Operation and Interagency Partnering, but should be implemented across the entire joint command structure. Further, fostering relationships at each level across partnering organizations provides avenues to develop personal connections among peers. These partners could be a community of people rather than organizations; the view should not be limited to organizations, as the most valuable partnership might be with a group of individuals.

Thirdly, another way organizations can work with partners to accelerate innovation is by breaking collaboration boundaries. To address rising societal and technological complexity, organizations need to look beyond traditional partners and conventional views on innovation for new inspiration and necessary capabilities. Organizations should explore unconventional partnerships and study nontraditional alliances emerging in other industries. There may be parallels with some industries that can integrate capabilities not commonly found in others. In a similar vein, one of the most difficult challenges is to think like a disruptor, as existing structures and governance models make it difficult to think beyond business as usual, especially when business as usual is working.

[7] Ibid., 49.

Disruptors question the norms and introduce new stimulation from the outside. Finally, it is beneficial to approach untenable issues or grand challenges by partnering across the entire system, namely with governments, non-governmental organizations or even with competitors.

## Partnership Models for the Co-creation of Public Services

Just as companies are involving customers in private sector innovation, governments are seeking to involve citizens. There is a growing trend to engage citizens in the co-creation of public services. Three broad issues have made it imperative for government agencies to change their relationship with citizens in problem-solving:

- Ongoing budgetary pressure motivates new, less resource intensive modes of problem-solving in government.
- The complex nature of the problems calls out for more collaborative approaches that involve external partners, including citizens.
- New technologies make connecting with citizens easier and reduce the cost of such collaboration in problem solving.[8]

The 2013 Study by the IBM Center for the Business of Government conducted by Satish Nambisan and Priya Nambisan outlines four distinct roles citizens can play in public service co-creation and problem-solving: explorers, ideators, designers and diffusers. As explorers, citizens can identify, discover and define emerging and existing problems in public services.[9] A good example of this is the e-People initiative in South Korea, which allows citizens to voice their concerns and ideas through e-petitions. The objective is to "make a new face of Korea by resolving even trivial complaints after listening closely to the voices of the people and accepting their creative ideas positively."[10]

As ideators, citizens can conceptualize novel solutions to well-defined problems in public service. Challenge.gov is an example of this. The initiative provides a listing of challenge and prize competitions, all of which are run by more than 80 agencies across the US federal government. As stated on the Challenge.gov website: "These include technical, scientific, ideation, and creative competitions where the US government seeks innovative solutions from the public, bringing the best ideas and talent together to solve mission-centric problems." Challenge.gov has offered more than $220 million in prize money since 2010.

Next, as designers, citizens are able to design and/or develop implementable solutions to well-defined problems in public service. For example, citizens

[8] Satish Nambisan and Priya Nambisan, *Engaging Citizens in Co-Creation in Public Services: Lessons Learned and Best Practices* (IBM Center for the Business of Government, 2013).

[9] Ibid.

[10] https://www.epeople.go.kr/jsp/user/on/eng/intro01.jsp.

may develop applications, or apps, based on open government data, as governments are adopting open data strategies to enable citizens to build innovative solutions. For example, data.gov.uk shows an extensive list of apps built on open data. The top rated app, Fasteroute, provides users with real time information about train departures and arrivals on the national rail network. The Route Risk app is another very useful app that analyses the safety of roads based on road safety data from the UK Department for Transport.

Finally, as diffusers, citizens may support or facilitate the adoption and diffusion of public service innovations among specific target populations. This is very similar to launching customers in the private sector.

The four roles imply different types of government vs. citizen interaction and thus require different approaches and mechanisms to support them. These approaches and mechanisms depend on the innovation ecosystem and the innovation platform.

## Innovation Partnership Models in Defense and Security

The citizen co-creation approach also has merits for the defense and security industry, although the sensitive nature of the problems and solutions limit certain government interactions. There are several examples of comparable strategies in the defense and security sector. One major example is the Network and Information Sciences International Technology Alliance (ITA) – a collaborative research alliance between the UK Ministry of Defence (MOD), US Army Research Laboratory (ARL) and a consortium of more than 20 leading academic and industry partners.[11] The ITA program started in 2006 with the strategic goal of producing fundamental advances in information and network sciences that will enhance decision-making for coalition operations, enable rapid, secure formation of ad hoc teams in coalition environments and enhance US and UK capabilities to conduct coalition warfare. The first phase of the ITA program concluded in 2011, and now the program is in its second phase. The ITA brings an extensive number of players together and focuses on specific defense issues. The outcomes of the research are available to all participating organizations and several findings made their way into the public domain in the form of an extensive list of published papers, so that organizations can take these findings forward into new products and solutions.

Meanwhile, the US Department of Defense (DoD) Defense Advanced Research Projects Agency has begun using InnoCentive as a platform for innovation.[12] InnoCentive@Work is collaborative innovation management software that enables organizations to engage diverse innovation communities such as employees, partners or customers to help rapidly generate novel ideas and solve the most pressing problems. Commercial organizations and government agencies use the platform to crowdsource challenges through collaboration

[11] http://www.usukita.org.

[12] http://www.innocentive.com.

with individuals, communities and networks. The DoD has also reached out to innovation from different sources opening offices in Silicon Valley in a project called DIUx. In the competitive and fast-moving technological environment, the DoD hopes "DIUx will help to cultivate and facilitate a lasting relationship with new innovators, initially in Silicon Valley, and those who don't always work with DoD, to help expand its innovative ecosystem of ideas."[13] The mission of DIUx Silicon Valley is to serve as a local point to strengthen existing relationships, build new ones and scout for breakthrough and emerging technologies.

Another example of partnership is Niteworks between the MOD, the Defence Science & Technology Laboratory (DSTL) and more than 150 UK-based companies that work together to support MOD decision-makers in the fields of operations, acquisition and capability.[14] Based on the success of the partnership, the initiative has been extended to 2018. The Niteworks approach enables the MOD to rapidly assemble expertise in an impartial environment, with access to prior knowledge and industry intellectual property from across the defense community. It brings together knowledge of the problem and solution space, which both enables a better understanding of the feasibility of recommendations and allows them to be rigorously tested and challenged from a range of perspectives, blending incumbent knowledge with the fresh thinking of new suppliers – be they generated by small and medium-sized enterprises or a global company.

Similarly, in 2010, 2012 and 2014, the Brussels-based think tank, Friends of Europe (formerly Security and Defence Agenda), conducted Security Jams to discuss global security.[15] This included brainstorming a broad range of security issues from security in Afghanistan to countering piracy operations and collaboration with emerging security players like China and India. These security topics were discussed in online forums and brought together a diverse set of thousands of security professionals from around the world. Each Security Jam resulted in a list of top ten recommendations for the NATO and EU leadership. The Security Jams are unique in the sense that they reach far beyond the usual suspects and discuss security matters in an unclassified, open environment.

## Challenges to Effective Public-Private Collaboration on Innovation

Numerous articles have been written about the issues and challenges of driving innovation through partnerships between government and industry.[16] The key obstacles from an industry perspective seem to involve the application of acquisition rules, a mismatch in corporate cultures and lagging timelines. The biggest issue with the acquisition rules is that the technology cycles far outpace

[13] diux.mil.

[14] niteworks.net.

[15] friendsofeurope.org.

[16] See, for example, http://www.govtech.com/local/4-Key-Challenges-Facing-Local-Government-Innovators.html

the acquisition timelines. Too often, industry must work with outdated requirements during the tendering process. While acquisition rules intend to safeguard a level playing field and equal opportunities for bidders, they also take away some of the motivation to get involved in the pre-competitive phase of the procurement, during which innovations and new technologies can be discussed; there is an incentive to wait for the acquisition to be published and avoid the costs involved in the collaborative phase before the tender.

However, it is important not to confuse activity with results, as these have different meanings for different stakeholders. Businesses express results in terms of innovation, revenues, profits and growth. Governments have a different set of metrics to judge output and results. This also means that risks are assessed differently by business leaders and governments. Government leaders should offer incentives for trying new approaches and, even better, for succeeding. Punishing failure will inhibit innovation. These differences in culture make public-private sector collaboration more difficult.

A mismatch in timelines and sense of urgency hampers collaboration as well, and especially precludes the involvement of small and medium-sized enterprises. The private sector operates against the cadence of the (financial) markets with a strong focus on the bottom-line. These issues are not easy to overcome, but a number of steps can be taken to improve the overall climate in which partnering and collaboration occurs. The first is to take a programmatic approach to partnering and collaboration. Governments interact with industry through multiple groups and stakeholders, which requires some level of coordination. It is simply too expensive for industry to keep collaborating in a haphazard way, especially if the timelines are long. The second step would be to communicate openly and often and create a feedback loop. It is crucial for industry to understand what has been done with the information which is received from the industrial partners; this is part of the incentive model. Feedback regarding what the government likes about certain recommendations is important, just as is the feedback what the government does not like. A third step would involve ceasing activities that do not lead to results. Industry faces less of a problem stopping operations than if it continues with activities that produce no results. A fourth helpful step would be to establish a governance mechanism with industry to discuss collaborative activities. This would involve treating the industrial sector as a real partner and bringing small and medium-enterprises on board.

## Recommendations and Policy Considerations to Overcome Innovation Challenges

While most government organizations are not concerned with market share or fending off competitors, they are focused on delivering services and operating in complex and dynamic environments where demand and the expectations of their constituents are increasing rapidly. As such, it is imperative for government organizations to create panoramic perspectives to better understand the complex operating environments (both physical and digital) in which they operate and to better understand the needs of their constituents.

The 2015 CEO Study[17] provides a clear set of recommendations about dealing with technologies and innovation:

### 1. Form your own futures squad

Set up a specialist forecasting team, equipped with the right technologies and skills. Recent research shows people trained to use probabilistic reasoning techniques, and recognize and eliminate bias, produce better forecasts. Working in teams likewise increases the odds of predicting the future accurately. Consider designating someone within your organization or agency specifically to scan for new technologies and monitor the marketplace.

Set up an innovation center outside the current organizational structure for incubating and piloting new business models and offerings. Give it the latitude to experiment properly, including sufficient time and resources. Test the most promising prototypes on a select group of knowledgeable, impassioned customers and constituents. And be ruthless about discarding all but the very best options.

### 2. Cultivate your cognitive capabilities

There's no technology that can tell you exactly what will happen in the future. However, using predictive and cognitive analytics to scrutinize the real-time data you receive from across your extended enterprise and mission area will help you forecast what might happen with a greater level of confidence. It will also enable you to generate "what-if" scenarios and risk assessments, allowing you to prepare for different outcomes before they occur.

### 3. Take an ecocentric view of the world

Concentrate on building broader networks and look at what organizations in unrelated industries are doing to get completely different ideas. Assess the caliber of all the organizations and enterprises in your ecosystem. Are you leveraging all their contacts, skills and assets? Are there any weak links? Are there any missing skills? Ask yourself whether your ecosystem has the right expertise to exploit new trends and technologies and boost its power to compete. If not, where should you look? The fate of your organization now rests on the collective abilities of the ecosystem in which you operate, including its ability to read—and prepare for—the future.

All recommendations depend on two essential enablers to deal with disruptive innovation in government organizations: an innovation ecosystem and an innovation platform. Without both, innovation will to fail.

The ecosystem or community of innovators from government agencies, non-profits and the private sector should come together and rally behind a common shared perspective of the operating environment. This community

[17] IBM Institute for Business Value, *Redefining Boundaries*, 29.

will not sustain itself unless it is supported by a platform and venue (physical and virtual) for innovation and problem-solving. An innovation platform provides the structure for knowledge exchange and facilitates the problem-solving process. Given the rate of unprecedented technological change, governments, militaries and businesses must find creative ways to work and innovate together as described above. The trick is to overcome the dominant logic or thinking in the defense and security industry and explore disruptive innovations.

## About the author

Leendert van Bochoven is member of the global leadership team for IBM´s Public Sector. He is the global lead for National Security, focused on serving clients in Defence, Intelligence and Public Safety. He is also leading IBM´s engagement with NATO and European Defence Agency.

In June 2015, Leendert became member of IBM´s Industry Academy. The Industry Academy was established during IBM´s centennial year (2011). The goal is to help increase IBM's industry capabilities internally, advance IBM's industry thought leadership and brand recognition externally, and connect transformative insights across industries to deliver client transformation.

Leendert is member of the Board of Directors of AFCEA and member of the American Defense Industries Forum in Brussels. He has a degree in Business Economics from the Erasmus University in Rotterdam, the Netherlands.
E-mail: L_van_Bochoven@nl.ibm.com

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

A.M. Ionescu, *Connections QJ* 15, no. 2 (2016): 31-47
http://dx.doi.org/10.11610/Connections.15.2.03

**Research Article**

# Nanotechnology and Global Security

*Adrian M. Ionescu*

*Ecole Polytechnique Fédérale de Lausanne, Switzerland, http://www.epfl.ch/index.en.html*

**Abstract**: Nanotechnology enables new solutions with numerous civilian and military applications. This paper provides an introduction to nanotechnology as a strategic research and industry field, presents trends with key potential impact and examines related policy and security implications. In lieu of conclusion, the author provides a number of policy considerations in regard to the security application of nanotechnology.

**Keywords**: key enabling technology, cyber-physical systems, research policy, dual use, prevention.

## Introduction

Nanotechnology refers to the creation of useful materials, devices and systems through manipulation of matter on the nanometer (nm) scale, with characteristic dimensions below 100nm, and exploiting of novel phenomena and properties specific to this small scale. In order to better understand the dimensional challenges for technology and materials, Figure 1 illustrates several objects associated with the aggressive scaling-down. It is remarkable, for instance, that today's 14nm Metal Oxide Semiconductor Field Effect Transistors (MOSFET) are smaller than a virus and form the core-switching device block for all modern nanoelectronics supporting high-performance and mobile computing. In fact, the manufacturing of ever-smaller and higher performance semiconductor devices entered the nano domain after the year 2000, with the introduction of the 90nm CMOS technology node, highlighting that nanoelectronics has been one of the very first technological domains to exploit atoms-to-systems approaches in industrial applications.

Even more important and fascinating with regard to nano is that the bulk properties of macro-scale materials could often change dramatically when their dimensions are aggressively scaled down. This concerns changes in their electrical, mechanical, optical and chemical properties by orders of magnitude, which led many researchers to call these nanomaterials "wonder materials."[1,2] One-dimensional (1D) and two-dimensional (2D) materials have a relatively larger surface area when compared to the same mass of material produced in a larger form and, when conducting electricity, they experience strong quantum effects. Their chemical reactivity could also change. Many of the nanoscale materials (carbon nanotubes [CNT], graphene, metal oxides, nanoceramics, etc.) become much stronger mechanically than predicted by existing material science models at the macroscopic scale. For instance, the Young's modulus of carbon nanotubes could be similar to the one of diamonds, and their thermal conductivity is enhanced by orders of magnitude. The causes of these drastic changes generally stem from the world of quantum physics. Understanding, modeling and controlling the property of matter of nanoscale to engineer new nanosystems and nanomaterials with unrivalled performance is one of the challenges of 21st-century science. Overall, nanotechnology can indeed also be seen as a platform of enabling techniques,[3] rather than a discipline-specific or materials-specific undertaking.

On the other hand, as nanotechnology concerns manipulations at atomic and molecular levels, and the creation of artificial objects with extreme properties at a scale invisible to the human eye, it raises controversy, especially related to its impact in the medical and environment fields. Science fiction scenarios involving self-replicating nanobots[4] endangering human life and fears related to nanobioengineered food (genetically modified) created some initial negative perception of nanotechnology. On the other hand, today's computer and mobile communication technologies already use nanotransistors in silicon chips and exploit quantum effects related with charge transport and storage for information processing in all hand-held devices, without posing any threats to the users. These greatly benefit from all the services enabled by nanocomputation.

In the long term, the true promise of nanotechnology, as anticipated by Ray Kurzweil, is that "we'll be able to create just about anything we need in the physical world from information files with very inexpensive input materials."[5] It

[1] Probably the best known two-dimensional "wonder" nanomaterial is grapheme, cf. www.europarl.europa.eu/news/en/news-room/20150603STO62104/Graphene-the-wonder-material-of-the-21st-century.

[2] Andrea C. Ferrari et al., "Science and Technology Roadmap for Graphene, Related Two-dimensional Crystals, and Hybrid Systems," *Nanoscale* 7/11 (2015): 4598–4810.

[3] J. Whitman, "The arms Control Challenges of Nanotechnology," *Contemporary Security Policy* 32:1 (2011), 99-115.

[4] Bill Joy, "Why the Future Doesn't Need Us," *Wired*, 1 April 2000, www.wired.com/2000/04/joy-2.

[5] "Ray Kurzweil on the Future of Nanotechnology," FUTURE TEK Science & Technology News, 20 September 2011, http://www.futuretek.info/ray-kurzweil-on-the-future-of-nanotechnology/.

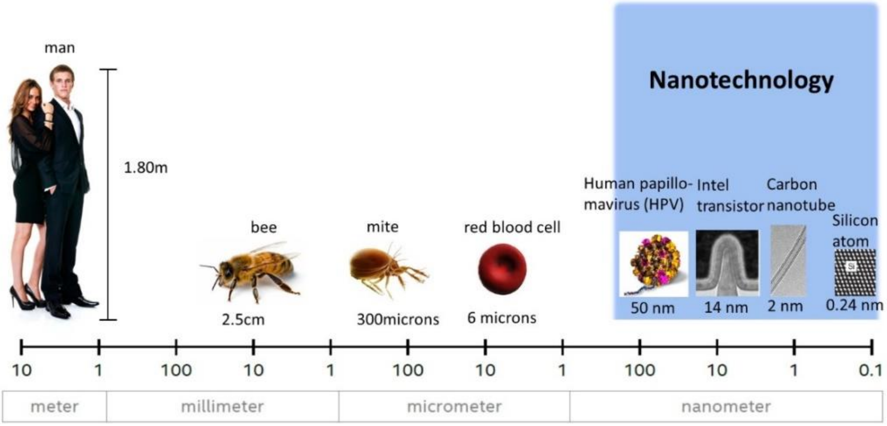


**Figure 1: Scale of dimensions from meter down to nanometer: the 14nm Intel transistor is today's most abundant artificial nanometer object ever created by humans.[6]**

is then obvious that nanotechnology is an immense opportunity for many security applications that no longer face the same limits posed by traditional technologies. Interestingly, when looking into the privileged nanotechnology research directions related to protection, survivability needs and extension of human senses, focusing on the soldier of the future [7] one may discover many convergent multi-use applications for firefighters, police officers, other first responders and the civilian community at large.

## Nanotechnology as a Strategic Research and Industry Field from a Security Perspective

The world is currently entering a new phase of information and communications technology (ICT) development that is expected to drive economic growth and sustainable development for the coming decades. In the future, people, systems and objects will interact seamlessly with each other in Internet of Things (IoT) scenarios. Nanotechnology is expected to be a key enabling technology (KET) to sustain the development of future smart sensing systems and/or Cyber-Physical Systems (CPS)[8] that will jointly integrate sensing, compu-

[6] Intel, 14 nm Technology, www.intel.com/content/www/us/en/silicon-innovations/intel-14nm-technology.html.

[7] Institute for Soldier Nanotechnologies, MIT, USA, http://isnweb.mit.edu.

[8] A cyber-physical system (CPS) is a system of collaborative computational elements controlling physical entities; they can be designed as networks of interacting elements with physical input and outputs and are expected to support future critical infrastructures, forming the basis of emerging and future smart services.

tation, communication and energy management functions. Nanotechnology is certainly the next industrial revolution and is expected to offer massive and unprecedented improvements in the following domains of society and the economy, and directly impact everyday life:

- *Energy efficient technologies* in all forms, starting from energy-efficient sensor networks for body and building monitoring as parts of smart cities[9] and smarter planet[10] concepts, to energy efficient high-performance computation in data centers. Essential to achieve this objective is a careful selection of basic nanotechnologies that can reduce the energy per computed, communicated and sensed bit, combined at the system level with novel generations of rechargeable batteries, energy storage devices and energy scavengers.
- *New inexpensive techniques for manufacturing and mass production* is one of the most interesting avenues of nanotechnologies exploiting bottom-up fabrication techniques and the use of new nanomaterials (nanowires, nanotubes, nanoparticles) in an independent way or in combination with existing materials to create objects with unique properties and performance.
- *Improved and sustainable solutions to enable nanohealth and longevity* together with a new quality of life.
- *Intelligent transportation* including electric auto, marine and rail and intelligent infrastructures as well as node-to-node interactions.
- *Improved safety, privacy and security*.
- *Healing and preservation of the environment* together with the reduction of the carbon footprint of human development and with novel solutions for better water and air quality.
- Push the limits of *space exploration* further.
- *Education*, which is expected to undergo dramatic paradigm changes, both in terms of format (new ways to better teach content) and the delivery (remote delivery of knowledge and facilitated lifelong education).
- Making *ICT available to all*, at the global scale, and contribute to the *spread of democracy and globalization* overall.

Therefore, nanotechnology becomes a strategic field of investment that cannot be neglected by any country and nation. Its fields of impact are much more numerous than some of the initially expected breakthroughs in information processing (related to high performance and ubiquitous computing) and in medicine.

The nanotechnology revolution will certainly impact both civilian and military applications that can no longer be considered independently and will cer-

[9] https://ec.europa.eu/digital-agenda/en/smart-cities.

[10] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/smarterplanet/.

tainly be confronted with a new set of great opportunities and associated risks. From a societal point of view, when it comes to considering nanotechnology's implications for privacy, security and human rights, this becomes a much more complex problem because it concerns a wide range of emerging fields, including nanomanufacturing, nanoassembly, information technology (including nanoelectronic systems and the IoT), nanobiotechnology, nanopharmaceuticals and nanotherapies.

As nanotechnology is still an emerging field, international communities and nations are still in the position to shape the best trajectory of nanotechnology and avoid any possible malevolent uses, especially in the fields of national and international security. The resulting challenges should be very well understood by fully engaging the scientific community to objectively assess both the enormous positive potential of nanotechnology as well as the necessary regulations to prevent any associated risks. It is then important for governments to fully understand the importance and impact of nanotechnology from the economic, societal, security and military perspective and exploit its full potential based on *preventive strategies* implemented at all levels.

## Trends in Nanotechnology: Present and Future

Despite tremendous recent progress, nanotechnology is just emerging from its infancy and experts are still far from taking full advantage of its expected economic and societal benefits. This section discusses the domains in which nanotechnology's technical progress is clearly related to new applications and services, even though its future could still be quite different.

### *Nanomaterials*

This field forms one of the largest segments, with a crucial role in the future all applications of nanotechnology. A "nanomaterial" has at least one of its dimensions in the range between 0.1-100nm: nanograins less than 100nm in size, nanowires, nanotubes or nanofibers less than 100nm in diameter, and films less than 100nm thick; at these dimensions they exhibit significantly improved or totally new behaviors and properties. There are many categories of nanomaterials with diverse uses and their categorization is relatively difficult. However, the following 12 categories have received particular attention in the last decade: (1) nanostructured materials, (2) nanoparticles and nanocomposites, (3) nanocapsules, (4) nanoporous materials, (5) nanofibers, (6) fullerenes, (7) nanowires, (8) single and multi-walled (carbon) nanotubes, (9) dendrimers, (10) molecular electronics, (11) quantum dots and (12) ultra-thin films. Electronic, mechanical and optical devices all directly benefit from the intrinsic nanomaterial properties in terms of combined performance and scalability.

### *Exaflop Energy-Efficient Computing*

Major initiatives to advance scientific computing are focusing on building exaflop supercomputers. In the United States, the National Strategic Computing

Initiative (NSCI) made strong demands on supercomputers to achieve incredible new levels of performance and power efficiency. Such exaflop supercomputers will be roughly 30 times more powerful than today's fastest machines, and their graphics processing units will be able to handle up to ten times more operations per unit of energy compared to present computers. This is why a great deal of focus is currently dedicated to exploring new energy-efficient nanotechnologies, capable of delivering the aforementioned performance and energy efficiency. Such exaflop computers would have the potential to provide unprecedented insights into many domains such as personalized medicine, human brain understanding, climate prediction, economic models and critical security issues. Concerning security, many experts believe that the defense capacity and strategy of any country will be strongly related to its future computing power.

### *Nanosensors, Smart Wearables and the Internet of Things*

The nanosensor field is one of several immediately and massively benefitting from nanotechnology, as the ultra-small size of these devices makes them very suitable to detect extremely small concentrations of gases or any types of particles, pushing their sensitivity to theoretical limits. Moreover, the nanofunctionalization of surfaces can solve major challenges of sensor selectivity and cross-talk as well as make sensors' surfaces self-cleaning or self-attachable. Nanosensors have such small power consumption that they can be powered by energy harvesters such as solar cells, thermoelectrical generators or from kinetic energy, their energy efficiency makes them suitable to be part of any future autonomous-sensing systems. Moreover, a large majority of nanosensors can be used in advanced nanoelectronics platforms that already have available nanodevices smaller than 22nm, which simply means that there is a high technology readiness level (TRL) for nanosensors of any kind, even though for industrial applications there is still a certain difference in their degree of maturity. Such sensors, based on a convergence of computing and sensing platforms, have been proposed and demonstrated recently.[11] Security applications such as electronic noses, nanobiosensors and all types of environmental sensing can greatly benefit from nanosensors. Today, sensors are key components and enablers of any complex scenarios that consider real-time extensions of the human senses in both civilian and military applications.

Advanced concepts related to their wearable embodiments have been proposed by the Future Emerging Technology Flagship project's Guardian Angels for a Smarter Life (GA project).[12] They have been foreseen as quasi-invisible, zero-power body area networks or, if appropriate, implantable devices, monitoring vital signs and offering the necessary information for taking appropriate

[11] Sara Rigante, et al., "Sensing with Advanced Computing Technology: Fin Field-Effect Transistors with High-K Gate Stack on Bulk Silicon," *ACS Nano* 9/5 (2015): 4872–4881.

[12] http://www.ga-project.eu.

action to preserve human health. They will acquire a well-defined view of the state of a person's health adapted to individual needs by using a real-time, ultra-low-power, multi-parametric combination of non-intrusive, bio-signal sensors (ECG, accelerometers, gyroscopes, pulse oximetry, etc.) to allow for early warning and thus enhancement of quality of life. They can employ emerging technologies such as electronic skin or wearable self-powered networks of sensors with wireless interfaces. These systems will be compatible, from the communication point of view, with all existing gateways (such as smartphones and smart watches) to serve as smart parts of a future vision of the IoT.

More sophisticated versions of such smart systems proposed by the GA project in Europe could protect people from diverse environmental dangers, including pollution and catastrophic events, rendering environments safer. These devices are expected to offer real-time access to an augmented reality including alerts for hazards, such as electromagnetic or ionizing radiation, extended UV exposure, concentration of allergens, pollens and harmful gases. They feature complex, energy-efficient communication technologies based on novel nanomaterials, offering complete networking capabilities. Environmental applications can be foreseen in many different approaches, such as sixth-sense smart air and water quality companions for indoors and outdoors and as trusted personal devices for complex disaster management.

### *Energy Harvesting, Storage and Management for Smart (Micro/Nano) Systems*

Nanotechnology is capable of addressing fundamental challenges involved in converting different forms of energy available in the environment (solar, thermal, chemical and mechanical) into electric energy, and efficiently storing and managing the converted energy to power future autonomous systems. According to the GA, solar cells could surpass the ultimate efficiency limit with new nanodevice architectures and new nanomaterials (such as exploiting multiple exciton generation). In thermal harvesters, room-temperature thermoelectric small-to-medium size devices with ZT systems significantly larger than 1 are possible with nanostructured materials, based on technologies including flexible materials, the integration of superlattices and quantum dot structures. Low and wideband nanoresonators made in arrays can increase the energy output of mechanical harvesting. In energy storage electrode devices with high area (nanotrenches, nanopillars, carbon nanotubes and graphene) a high conductivity are taking full advantage of the 2D and 1D nanostructures.

### *Authentication*

Authentication is a crucial component in network security and will certainly be impacted by developments in nanotechnology. Improving the accuracy associated with authentication is one expected future outcome. Although nano-optics is considered potentially useful for the most sophisticated security authentication techniques, with the advancement of nano-enabled multi-parameter sensors, authentication may in the future include sophisticated access keys based on individualized multi-parameter techniques, including biological signals, which would be difficult to reproduce.

### *Quantum Cryptography*

Today's cryptographic algorithms are based on key encryption and related algorithms that are considered secure enough. Meanwhile, quantum computers are based on qubits and require information processing at the atomic level, an emerging technology that made a great deal of progress in last decade. These computers will not replace current computers for any type of computation, but can offer fantastic opportunities for complex pattern recognition and novel unbreakable encryption techniques. If quantum computing becomes a reality, it will reengineer and dramatically change all the current cryptographic systems. However, one major threat is that quantum computing can also be used to break today's security strategies by reverse computing private keys faster than a conventional computer. For instance, it is estimated that 2048-bit RSA keys could be broken on a quantum computer comprising 4000 qubits and 100 million gates.

It appears that intelligence agencies are very concerned about this issue and, recently, the US National Security Agency (NSA) revealed interest in a transition to quantum-resistant protocols. The Dutch General Intelligence and Security Service singled out a different type of urgent threat in a scenario called "intercept now, decrypt later,"[13] whereby an attacker could begin intercepting and storing financial transactions or other sensitive encrypted traffic and then unscramble it later, once a quantum computer becomes available. This field is even more relevant given the recent progress on increasingly successful qubit implementations in silicon nanotechnology,[14] capable of upscaling quantum computers and bringing them to fruition within 20 years.

### *Regenerative Medicine and Molecular Engineering*

One of the main goals of the multi-disciplinary efforts related to regenerative medicine is to fabricate biological mimetic nanoscale scaffolds to repair and replace damaged biological tissues. Cell sources and biological signals have become the gold standard of tissue engineering, while the use of micro-nanofabrication techniques to generate scaffolds to guide stem/progenitor cell adhesion, spread, differentiation and migration constitute emerging fields in tissue engineering and regenerative medicine. A key aspect concerns the fact that "understanding interactions of nanomaterials with stem cells may provide knowledge applicable to cell-scaffold combinations in tissue engineering and

[13] Chris Cesare, "Online Security Braces for Quantum Revolution," *Nature* 525 (8 September 2015): 167–168.

[14] Menno Veldhorst et al., "A Two-qubit Logic Gate in Silicon," *Nature* 526 (15 October 2015): 410–414.

regenerative medicine."[15] Moreover, the design of reliable scaffolds with low toxicity, controlled 2D surfaces for cell adhesion and assembly in a 3D structures are current challenges. In the future, combinations of sophisticated nanomaterials with progenitor or stem cells and proper biological signals are expected to provide further opportunities to support fully regenerative nanomedicine.

Anti-aging therapy and drug delivery involve molecular engineering and the injection of nanoscale machines in the bloodstream to target and repair or destroy cancer cells or address other pathologies. Cancer treatment is a key field where disruptive solutions are expected from nanoparticles that can be steered to uniquely target cancerous cells by embedding the delivery of nanoagents or other types of mechanisms for cancer cell destruction. In the future such cancer nanotherapies are expected to replace heavily aggressive chemo and radiation therapies.

Beyond any speculation about any significant extension of the human lifespan towards limits that are not imaginable today (more than 200 years or so), being frequently foreseen as steps towards immortality by anti-aging nanotherapy, there is strong hope that nanotechnology will advance truly regenerative approaches for tissues and organs, opening new paths for the medicine of the future.

### *Productive Nanotools with Atomic Precision*

Nanotechnology progress is expected to offer paths towards so-called atomically precise manufacturing (APM) and atomically precise productive nanosystems (APPNs). Today, the prototype-scanning probe-based APM systems that exist are evaluated in research labs, where they serve the prototyping and exploration of nanodevices and nanobjects. The semiconductor industry already possesses the technological tools for building the ultra-clean, thin layers of materials needed in nanoelectronics (such as atomic layer deposition, tools). Nanoscale APPNs come directly from nature and fabricate uniquely complex atomically precise nanostructures in enormous quantities. It is important to note that this field is of high importance for both organic and inorganic production, even though many of the production tools were initially foreseen for bioengineering.

## Nanotechnology Roadmaps

Europe and the United States are key contributors to establishing nanotechnology roadmaps and coordinating priorities for major investments in the field. The funding of military nanotechnology makes up a substantial share of total funding in the United States, which is the leader in this field and has been en-

[15] King-Chuen Wu et al., "Nanotechnology in the Regulation of Stem Cell Behavior," *Science and Technology of Advanced Materials* 14 (2013) 054401, doi: 10.1088/1468-6996/14/5/054401.

gaged in nanotechnology since the 1980s. Moreover, in 1996 nanotechnology was established as one of six strategic research areas for US defense. Accordingly, between 25 and 30 % of the US National Nanotechnology Initiative funding has gone to the US Department of Defense (DoD). The US military research and development in nanotechnology focuses on the development of miniature sensors, high-speed processing, unmanned combat vehicles, improved virtual-reality training and the enhancement of human performance.

In Europe, the focus is rather on the civilian application of nanotechnology, and the recent NANO*futures* report proposes a so-called value chain-based roadmap for nanotechnology, in which seven nanotechnology vectors are related to various application domains where industrial and economic impacts are foreseen.[16] Each of these vectors has relevant multi-sectorial impacts at different points in time, with the overall picture depicted in Figure 2. This report suggests that political and economic decision-makers should take action to address industrial needs and research and innovation challenges for the successful development of safe and sustainable nano-enabled products. The report contains numerous examples, potential leading markets and the societal challenges that can be addressed by nanotechnology markets, which served as basis for some of the funding plans decided in the European Horizon 2020 program. The so-called *inclusive, innovative and secure society* is part of the main societal challenges of this visionary roadmap.

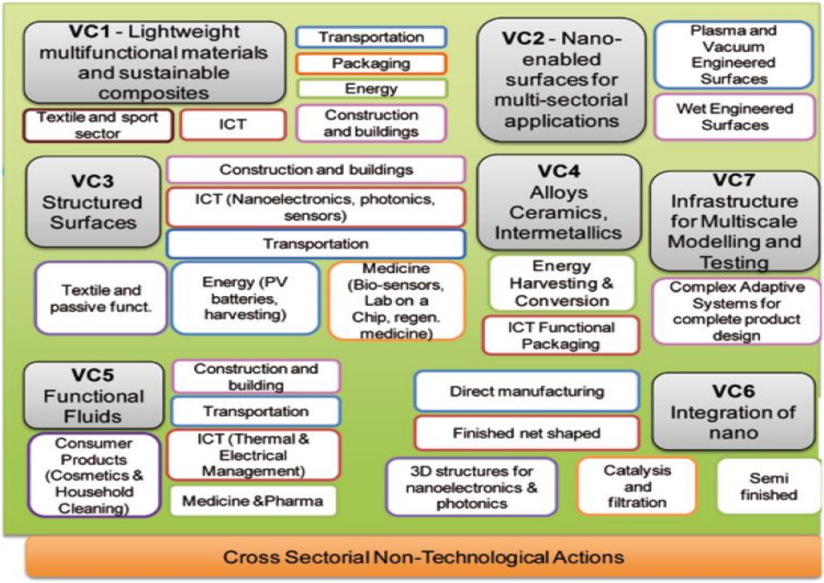
In the US, the Foresight Nanotech Institute, funded by the Waitt Family Foundation and Sun Microsystems and with the support of a multi-disciplinary group of scientists and engineers, created another nanotechnology roadmap.[17] Their vision is broad, including applications in medicine, biomedicine, new generations of sensors, computer technology, display and lightning systems. A particular focus is on molecular nanotechnology. This roadmap includes an interesting categorization and discussion of various nanotechnology domains in three horizons of time.

NASA's nanotechnology roadmap, meanwhile, is extremely detailed, and divided into four main sections in the Technology Area Breakdown Structure (TABS) for Nanotechnology, all with advanced specifications and challenges for space exploration:

i. *Engineered materials and structures*, divided into: (a) lightweight structures, dealing with nanomaterials for lightweight, durable structural systems and high-efficiency data cables, wiring and devices, (b) damage-tolerant systems, enhancing system robustness through improved interlaminar interfaces, health monitoring and built-in repair mechanisms, (c) coatings, constituted by very thin, engineered surface barriers that offer pro-

[16] *Integrated Research and Industrial Roadmap for European Nanotechnology* (Nanofutures, 2012), www.nanofutures.eu/sites/default/files/NANOfutures_Roadmap%20july%202012_0.pdf.

[17] "How Close Are We to Real Nanotechnology?" *Humanity+*, June 1, 2009, http://hplusmagazine.com/2009/06/01/how-close-are-we-real-nanotechnology.



VC1 - Lightweight multifunctional materials and sustainable composites

Transportation

Packaging

Energy

Textile and sport sector

ICT

Construction and buildings

VC2 - Nano-enabled surfaces for multi-sectorial applications

Plasma and Vacuum Engineered Surfaces

Wet Engineered Surfaces

VC3 Structured Surfaces

Construction and buildings

ICT (Nanoelectronics, photonics, sensors)

Transportation

Textile and passive funct.

Energy (PV batteries, harvesting)

Medicine (Bio-sensors, Lab on a Chip, regen. medicine)

VC4 Alloys Ceramics, Intermetallics

Energy Harvesting & Conversion

ICT Functional Packaging

VC7 Infrastructure for Multiscale Modelling and Testing

Complex Adaptive Systems for complete product design

VC5 Functional Fluids

Construction and building

Transportation

ICT (Thermal & Electrical Management)

Consumer Products (Cosmetics & Household Cleaning)

Medicine &Pharma

Direct manufacturing

Finished net shaped

VC6 Integration of nano

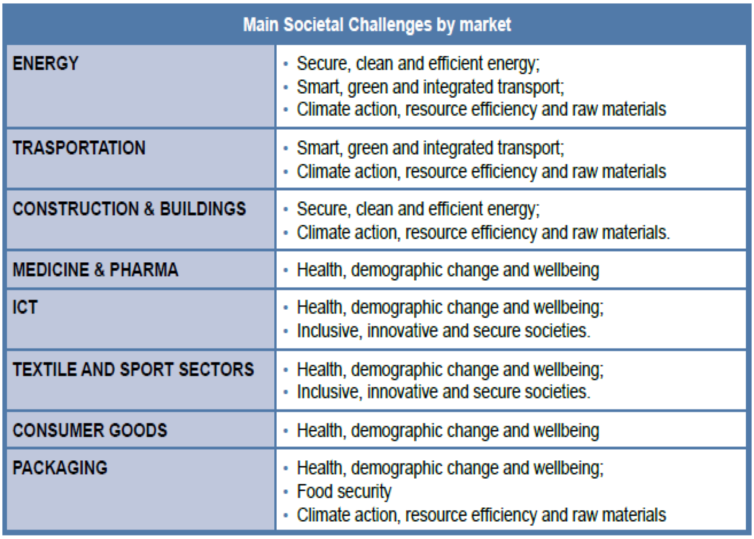
3D structures for nanoelectronics & photonics

Catalysis and filtration

Semi finished

Cross Sectorial Non-Technological Actions

(a)



| Main Societal Challenges by market | |
|---|---|
| ENERGY | • Secure, clean and efficient energy;<br>• Smart, green and integrated transport;<br>• Climate action, resource efficiency and raw materials |
| TRASPORTATION | • Smart, green and integrated transport;<br>• Climate action, resource efficiency and raw materials |
| CONSTRUCTION & BUILDINGS | • Secure, clean and efficient energy;<br>• Climate action, resource efficiency and raw materials. |
| MEDICINE & PHARMA | • Health, demographic change and wellbeing |
| ICT | • Health, demographic change and wellbeing;<br>• Inclusive, innovative and secure societies. |
| TEXTILE AND SPORT SECTORS | • Health, demographic change and wellbeing;<br>• Inclusive, innovative and secure societies. |
| CONSUMER GOODS | • Health, demographic change and wellbeing |
| PACKAGING | • Health, demographic change and wellbeing;<br>• Food security<br>• Climate action, resource efficiency and raw materials |

(b)

**Figure 2: (a) Value chains for nanotechnology, and, (b) the main societal challenges by markets, according to Nanofutures.[11]**

tection from environmental hazards and thermal management, (d) nano-adhesives for in-space assembly, and (e) thermal protection and control in extreme conditions.

ii. *Energy storage, power generation and power distribution*, which take advantage of processes that occur on the molecular and atomic levels for increased efficiency in the storage, generation and distribution of energy. Batteries and supercapacitors with high energy and power densities that use nanomaterials are expected to sustain reliable energy management functionality in harsh environments (extreme temperatures, radiation, reactive atmospheres).

iii. *Propulsion* is crucial to in-space propulsion needs, and NASA is looking into nanoparticle-derived propellants, propellant-free solutions and the use of nanomaterials with improved strength, thermal conductivity and reliability for lighter, efficient and long-life propulsion systems for space and aircraft.

iv. *Sensors, electronics and devices* have particular requirements in this case, with special emphasis on better performance, lower power requirements, greater packing efficiency due to smaller volumes and radiation hardness. These requirements are applicable to nanoelectronics, nanosensors, nanoactuators and various types of nanoinstruments.[18]

It is worth noting that many of the requirements for space exploration are of high relevance for military applications, as military technology may be deployed in space. In the past, the extreme specifications of space programs and airborne applications have triggered tremendous progress in civilian applications and the emergence of technological breakthroughs; this may be also related to the fact that performance and security criteria prevail over cost in this specific field, as it is mostly based on problem-solving approaches, in contrast to many other fields.

Summarizing all these trends into a common vision for a unified roadmap for nanotechnology with particular focus on security issues is a complex task given the large variety of nanotechnology domains, applications and degrees of maturity. Figure 3 depicts a possible scenario that foresees three major scenarios for nanotechnology-enabled security.

*Horizon I involves digital and nanosensing-enabled security*. Computing technology is already in the nanotechnology age, and is expected to deliver exceptionally high computation power in both mobile and fixed-infrastructure supercomputers when reaching sub-7nm gate transistors on advanced silicon CMOS platforms and with energy-efficient devices and system architectures. On top of similar nanoplatforms, the functional diversification in terms of multi-parametric nanosensing and nano-optics functions will advance authentication techniques and the early detection of any external dangers and hazards in civil society and in military environments. Everyday objects could be equipped with wearable physical, physiological and environment sensors that will act as extensions of the senses and as guardians of health by anticipating

[18] *NASA Technology Roadmaps – TA 10: Nanotechnology* (NASA, May 2015), www.lpi.usra.edu/sbag/goals/capability_inputs/2015_Tech_10_nanotechnology.pdf.

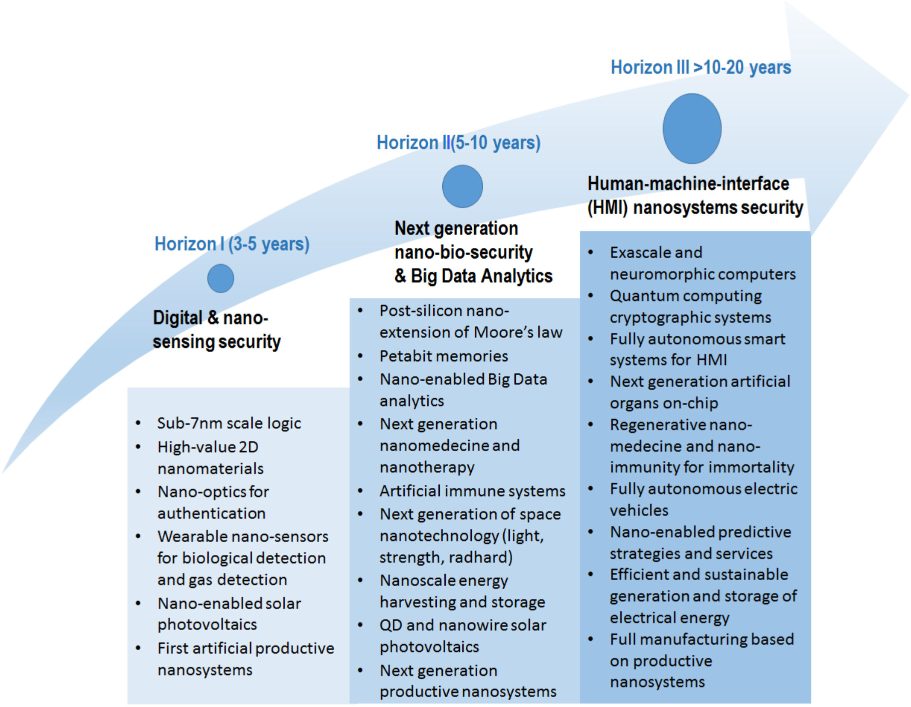

Horizon I (3-5 years)
Digital & nano-sensing security
Sub-7nm scale logic
High-value 2D nanomaterials
Nano-optics for authentication
Wearable nano-sensors for biological detection and gas detection
Nano-enabled solar photovoltaics
First artificial productive nanosystems
Horizon II(5-10 years)
Next generation nano-bio-security & Big Data Analytics
Post-silicon nano-extension of Moore's law
Petabit memories
Nano-enabled Big Data analytics
Next generation nanomedecine and nanotherapy
Artificial immune systems
Next generation of space nanotechnology (light, strength, radhard)
Nanoscale energy harvesting and storage
QD and nanowire solar photovoltaics
Next generation productive nanosystems
Horizon III >10-20 years
Human-machine-interface (HMI) nanosystems security
Exascale and neuromorphic computers
Quantum computing cryptographic systems
Fully autonomous smart systems for HMI
Next generation artificial organs on-chip
Regenerative nano-medecine and nano-immunity for immortality
Fully autonomous electric vehicles
Nano-enabled predictive strategies and services
Efficient and sustainable generation and storage of electrical energy
Full manufacturing based on productive nanosystems

**Figure 3: Roadmap of main present and future major trends in nanotechnology in three-level horizon, with relevance for security.**

risks and conditions in dynamic environments. Nanostructures will improve the efficiency of solar photovoltaics from solar panels to wearable photovoltaics, from outdoor sunlight to indoor low light intensity conditions. Energy sources will start to become part of some electronic systems, thereby enhancing their autonomy.

*Horizon II involves next-generation nano-biosecurity and big data analytics*. After digital computing technology, based on von-Neumann architectures, reaches saturation in terms of extreme scaling and energy efficiency, a post-silicon era will emerge with novel nanomaterials in the 3D form of multi-functional electronics chips, with many of them having more than computational (logic and memory) functions, such as embodied energy storage and analog-sensing features on the digital chip. Memory technologies will drive electronics further to meet the high demands of information storage, and the resulting big data will dominate the way applications and services are handled. This will generate enormous opportunities and challenges for both civilian and security-related applications, as networks of sensors will be deployed on large scales in smart city scenarios and in the implementation of environmental strategies. The (nano) sensors networks will be key parts of any battlefield strategy, together with smarter drones and visualization techniques, to provide a dynamic full map of hostile environments and use predictive big data analytics. This period of time will also see the emergence of nanomedicine and the generalization of the use of nanotherapies for cancer and other disease treatments. Being able to control, manipulate and build artificial systems at the nanoscale will push the frontiers of medicine, but at the same time generate the need for regulations and security approaches for nano-bio dangers not only for the battlefield, but also for the avoidance of terrorist attacks of a different kind, capable of impacting large populations. Nano-enabled energy management on all scales and nanoproductive systems will become more common in this period, and advanced nations will begin to implement fossil fuel industrial and transportation strategies for enhanced sustainability.

*Horizon III, called the human-machine-interface (HMI) nanosystems security,* concerns a long-term vision characterized by exascale computing capabilities, energy efficient neuromorphic and quantum computing for secure encryption and communications. In medicine, nano-enabled regenerative techniques will be used to extend life and the quality of life beyond currently imaginable limits. Society will benefit from the support of fully autonomous systems and cyber-physical systems in every sector of life. Thanks to nanotechnology, HMIs will reach a high level of sophistication, extending all human capacities. Society's dependency on fossil fuels will end, leading to a transformation into a clean and sustainable civilization that rather relies on smart electric vehicles. In the most optimistic scenario, humanity will learn how to use information technology and nanotechnology to propagate democracy and achieve a new quality of life. The medical field will become fully sustainable and implement predictive and personalized medicine. The big data collected with advanced autonomous multi-parameter systems with embedded self-repair features and subsequent data analytics will support the optimization of industrial processes. In an energy efficient society with sophisticated levels of security, threats can be predicted and not only monitored. Military strategies for potential conflicts could experience dramatic changes, raging shifting from the deployment of an invulnerable universal soldier or drones using nanotechnology merely to enhance traditional actions, to completely new strategies on the battlefield, where a multitude of actions and counteractions and their effects can be foreseen and evaluated with high levels of accuracy.

## Policy and Security Implications

The global policy context is very complex in the post-Cold War period, the rise of globalization and of Asia's economic power, the increase and aging of the global population, climate and resource problems, sustainability issues for healthcare in advanced industrialized states and security threats related to terrorism. In the past, technology was a servant of policies; today, there is major change because of economic wealth and growth. Policies and conflicts are thus heavily dependent on technology, which strongly influences political decisions from the very early stage. This can be viewed in some cases as a competition over the degree to which the developed world invests in research and nanotechnology. Even if such investments are seen by some as diverting government resources from social programs into "wasting" funds on advanced research on technology, this perception fails to objectively evaluate the long-term benefits for humanity even if only a few of the nanotechnology applications come to fruition.

European Union research is embracing an "integrated, safe and responsible" approach to nanotechnology.[19] This does not only concern nanomaterials, nanoengineering for productive systems, nanosystems and nanomedicine, but there are dedicated funding streams supporting nanotoxicological efforts and activities exploring the ethical aspects of nanotechnology, with the consideration of potential adverse effects on human health and the environment. Such an anticipatory approach of assessing both the benefits and risks of nanotechnology is very useful and is viewed in Europe as a basis for wider regulatory efforts at the European level.

During a talk at the California Institute of Technology in 2000, President Bill Clinton showed strong political insight into the importance of nanotechnology-related impacts on real life in the long term, with arguments that as appeared to be a political extension of Richard Feynman's scientific visionary speech. Clinton outlined the ambitions of what was the start of the field of nanotechnology supported by national policies:

> Just imagine, materials with 10 times the strength of steel and only a fraction of the weight; shrinking all the information at the Library of Congress into a device the size of a sugar cube; detecting cancerous tumors that are only a few cells in size. Some of these research goals will take 20 or more years to achieve. But that is why—precisely why—as Dr. Baltimore said, there is such a critical role for the federal government.[20]

The foundations and long-term views embedded in this speech remain valid to this day.

Finally, if there is any foreseeable security or conflict threat resulting from the competition between human expansion and the planet's limited resources, nanotechnology is among the very few credible solutions to this challenge. If there is any hope for economic sustainability at the global level and for worldwide security, nanotechnology is again one of the key answers.

[19] European Commission, *Nanotechnology: The Invisible Giant Tackling Europe's Future Challenges* (Luxembourg: Publication Office of the European Union, 2013).

[20] President Clinton‘s Address to CalTech on Science and Technology, The White House, Office of the Press Secretary (Los Angeles, CA, 21 January 2000), p. 3, available at http://caltechcampuspubs.library.caltech.edu/2676/1/nano_clinton.pdf.

## Recommendations and Policy Considerations for More Security with Nanotechnology-enabled Applications

The recommendations made in this section are solely based on the view of the author as an academic researcher in the field of nanotechnology and nanoelectronics, rather than someone with an engineering background.

*Recommendation 1: How to use nanotechnology to concretely devise solutions to global challenges – health, energy, climate change and security*. Nanotechnology has the unique potential to address global challenges, but very often its full potential is not leveraged. Given the diversity of nanotechnology fields, to maximize its nano's success as a truly disruptive option within a reasonable timeframe, it is recommended to structure a nanotechnology research and development (R&D) approach as a focused combination between top-down (*problem-solving oriented*) and bottom-up (*development of a generic technology, creating its own applications*) strategies and by involving multi-disciplinary teams. National agencies involved in R&D should realize that nanotechnology is a field that does not necessarily match the traditional structure of research units and approaches, and thus necessitates the different management of scientific approaches.

*Recommendation 2: How to make wireless sensor networks (WSN) and big data analytics game-changers for security*. In the short term, nanotechnology can enable wireless sensor nodes with multi-parameter sensing and long-term autonomy. Sensor networks that exploit nanotechnology are strategically beneficial to security because they generate a dynamic perception of the environment with very early detection of threats by analyzing big data available in real time. For security, this technology is deployable at different levels, including from humans (body area networks) to buildings, cities and large environments. Energy efficiency and scalability are the key features and priorities on which to concentrate to have this technology operational in the short term. It is recommended to particularly enhance the technology that transfers specific security programs using big data from WSNs for prevention in security, such as to prevent terrorist attacks. Additionally, wearable embodiments of WSNs can provide battlefield evaluations of the medical status of soldiers by evaluating in-situ the severity of injuries and preparing the most effective treatments.

*Recommendation 3: How to push the frontier of medicine with nanotechnology with a main emphasis on cancer and brain disorders*. There is still stringent demand for personalized medicine and finding new treatments concentrating on molecular technology; the potential of nanotechnology in this field is unique, but requires a paradigm change in medical research. Beneficial here would be focused roadmapping and a milestone-based approach for the advancement and take-up of nanotherapies, considering both their benefits and potential threats. The recommendation is to consider, from a political perspective, a massively concentrated effort on two key applications: cancer nanotherapy and the nanomonitoring and nanotherapy of brain disorders, two strategic domains with limited solutions. The study and understanding of brain disorders can have important implications for security as well.

*Recommendation 4: Early regulations and anticipatory efforts for nanosecurity*. As per European strategies, early regulations and anticipatory efforts are beneficial for the changing field as a whole; this concerns both the hardware (technological implementation) and big data layer (data security and privacy). It is recommended to address such regulations and dedicate anticipatory efforts in the field of nanotechnology for security, with embedded nanoethics principles, as a high priority for future society. This aspect is even more important because the military uses of nanotechnology are no longer considered independently of other uses in civilian life. Possible misuses should be at least addressed in regulations related to the general problem of the pace of human adaptation to new emerging technologies.

*Recommendation 5: How to avoid a nano-divide as a potential booster of inequality, tensions and sources of international conflicts.* As many countries seem to witness an ICT divide that correlates with inequality in the distribution of wealth, society should avoid allowing such a gap to be exacerbated by nanotechnology and being transformed in the long term into a new potential source of future conflicts of inequalities. Therefore, it is recommended that highly-industrialized countries identify such transitions policies from a *pre-nano* to a *post-nano* world from a very early stage.

## About the authors

**Adrian Mihai Ionescu** is a full Professor at the Swiss Federal Institute of Technology in Lausanne (EPFL). He received the B.S./M.S. and Ph.D. degrees from the Polytechnic Institute of Bucharest, Romania and the National Polytechnic Institute of Grenoble, France, in 1989 and 1997, respectively. He has held staff and/or visiting positions at LETI-CEA and LPCS-ENSERG, Grenoble, France and Stanford University. He is director of the Laboratory of Micro/Nanoelectronic Devices (NANOLAB). He is appointed as national representative of Switzerland for the European Nanoelectronics Initiative Advisory Council (ENIAC) and member of the Scientific Committee of CATRENE. Dr. Ionescu is the European Chapter Chair of the ITRS Emerging Research Devices Working Group.
*E-mail*: adrian.ionescu@epfl.ch.

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Filippa Lentzos, *Connections QJ* 15, no. 2 (2016): 48-64
http://dx.doi.org/10.11610/Connections.15.2.04

**Research Article**

# Biology's Misuse Potential

*Filippa Lentzos*

*Department of Social Science, Health & Medicine, King's College London*
*http://kcl.ac.uk*

**Abstract**: The international community has laid down clear red lines about the use of biology to enhance national armaments. Advances in bioscience and biomedicine are, however, significantly eroding technological barriers to acquiring and using biological weapons. This article describes recent scientific trends and analyses their security implications. Three emerging fields of research that have particularly high potential for misuse are considered in more detail: potentially pandemic pathogens, synthetic biology and neurobiology. It is argued that continued efforts are required in multilateral, national and scientific spheres to strengthen the red lines and to foster responsible science.

**Keywords**: Biological weapons, potentially pandemic pathogens, synthetic biology, neurobiology, disarmament, non-proliferation, biosecurity, responsible science.

## The Misuse of Biology

The international community has laid down clear red lines about the misuse of biology. The two biological cornerstones of the rules of war are the Biological Weapons Convention (BWC) and the Geneva Protocol. Together, they prohibit the development, production, stockpiling and use of biological weapons. Signed in 1972 and 1925 respectively, the two treaties have incorporated a mix of legal, diplomatic and political elements into the structure of international norms that are increasingly difficult to dismantle, ignore or override.

Scientific advances in biology and biomedicine are, however, significantly eroding technological barriers to acquiring and using biological weapons. This article describes recent trends in bioscience and analyses their security implications. Three emerging fields of research that have particularly high potential for misuse are then considered in more detail. Continued efforts are required in multilateral, national and scientific spheres to strengthen the red lines. Crucial areas to strengthen are (1) the international legal framework regulating biological weapons, (2) the BWC science and technology review procedure and (3) norms of transparency and public accountability.

## Trends in Bioscience

There are four frequently cited security-related trends in the biological sciences:[1]

1. The *increasing pace of advances* in bioscience. Rapid advances on multiple fronts within the life sciences pose challenges for tracking and assessing that progress in terms of what it means for biological weapons development. It is difficult to establish which areas to monitor, to anticipate what new combinations of advances will result from progress in multiple fields and to expand the types of expertise required to assess new developments.
2. The *increasing convergence* of biology and biomedicine with chemistry, engineering, mathematics, computer science and information theory. These developments are, for instance, enabling both the chemical synthesis of biological molecules and the biological synthesis of chemicals. Where components are significantly different from existing biological systems, or where inorganic materials mimic biological function and thereby have biological effect, the mechanisms of action of weapons might not be clearly "biological" or "chemical" – blurring the domains of the Biological and Chemical Weapons Conventions.
3. The *increasing diffusion of capacity* in biology and biomedicine around the world, particularly in emerging economies such as China and India. There are also increasing international collaborations, not only among researchers in scientifically developed countries and between researchers in developed and developing countries, but among regional networks and increasingly among scientists within developing countries.

[1] "The Biological and Toxin Weapon Trends Symposium," IAP Global Network of Science Academies conference, 13–15 September 2015; and "Assessing the Implications of Advances in Science and Technology for the BTW 2016," IAP Global Security Working Group Meeting, 16 September 2015, Polish Academy of Sciences, Warsaw, Poland (a summary is available at iapbwg.pan.pl); Organisation for the Prohibition of Chemical Weapons, *Convergence of Chemistry and Biology: Report of the Scientific Advisory Board's Temporary Working Group* (The Hague: OPCW, 2014); National Research Council, *Life Sciences and Related Fields: Trends Relevant to the Biological Weapons Convention* (Washington, DC: National Academies Press, 2011); "The Biological Weapon Convention Seventh Review Conference," 5–22 December 2011, Geneva, "New Scientific and Technological Developments Relevant to the Convention" (BWC/CONF.VII/INF.3).

4. The *increasing opening up of science* with new tools like wikis, blogs and microblogs altering how information is gathered, handled, disseminated and accessed; and amateur communities, scientific outreach and educational toys increasing access to hardware for wet work in the life sciences. A large number of multinational suppliers now produce kits containing reagents, enzymes and step-by-step instructions to conduct many of the basic lab techniques life scientists use, including nucleic acid and protein expression, purification, detection and analysis. Commercial services are also available for tasks like sequencing, DNA and protein synthesis, microarray construction, mass spectrometry analysis and others. The availability of smaller, more automated and easier to use bioinstrumentation also facilitates the performance of lab research.

## Impact on Bioweapons Potential

The trends in bioscience are making it easier to develop biological weapons. The most recent assessment by the global network of science academies concludes that technological barriers to acquiring and using bioweapons have been significantly eroded over the last five years.[2]

It is now easier to acquire both natural and synthetic pathogens and to enhance and optimize them for specific purposes, including for use in biological weapons. It is also easier to produce biological agents. Critical lab equipment such as reaction vessels (including those currently covered by control lists) can now be fabricated using 3D printing technology. The increased use of biosynthesis and bio-based production, scaffolds and "biopharming" has accelerated the speed and yield of biological agent production. In addition, the space and resources required for biologics production has decreased and the physical size of production equipment has been drastically reduced. Less space and time are now required for scale up, and it is easier to conceal nefarious activities. Advances in nanotechnology and aerobiology, along with the use of chemical co-factors to increase uptake and formulations to improve absorption from the gastrointestinal tract, are making the dispersal and delivery of biological agents easier, and increasing antimicrobial resistance is complicating the administration of prophylactics. In short, the global network of science academies argues that scientific advances "could facilitate almost every step of a biological weapons programme."[3]

While the risks of small-scale bioterrorism attacks are real and present, the likelihood that scientific advances will be used to "enhance" these attacks is relatively low – many of the cutting-edge developments are expensive and

[2] "The Biological and Toxin Weapon Trends Symposium."

[3] Ibid.

complicated to acquire and deploy successfully.[4] Instead, the most significant security threat from the misuse of advances in the biological sciences comes from sophisticated biological attacks from professional and well-resourced institutions like national militaries.[5] This is backed by the historical record of both biological weapons development and bioterrorism incidents.[6]

The international community has committed itself—through the BWC and the Geneva Protocol—to take precautions that scientific developments are not misused. Over the life span of the BWC, there has been no state party use of biological weapons, and most experts agree that the potential for state use is very low.[7] There are various reasons cited for this: biological weapons are not considered "good" weapons; it is difficult to produce sophisticated and reliable biological weapons and it is not politically viable to use them because the norm against biological warfare—encoded in law through the BWC—is exceptionally strong.

Yet, while the norm against biological weapons is strong, and the potential for state use is very low, a blanket rejection of the bioweapons threat from states is dangerous. It cannot be assumed that biological weapons will not be used in the future, and the likelihood that they will be used is not zero. Although twentieth-century military use of biological weapons was envisioned primarily as strategic and came to rest on delivery by bomb, missile or large area spray, there were also scientists and military planners who seriously entertained other ideas, such as tactical use and sabotage. One must not necessarily think of biological weapons today as in the twentieth century. Biological warfare can, for instance, be compared with cyber warfare in that the victim may know it has been attacked, but not by whom, or it may not know or be able to prove that it has been attacked at all – the question of who is to blame might not even be asked. The silent and invisible nature of biological weapons could, for instance, make them highly potent means for weakening the legitimacy of enemy regimes within their own populations, or for just keeping them busy. In the "best case" scenario it may be possible to actually get rid of enemy regimes without anyone recognizing foul play.

[4] Filippa Lentzos, "The Risk of Bioweapons Use: Considering the Evidence Base," *BioSocieties* 9:1 (2014): 84–93; Catherine Jefferson, Filippa Lentzos, and Claire Marris, "Synthetic Biology and Biosecurity: Challenging the 'Myths',''  *Frontiers in Public Health* 2:115, http://dx.doi.org/10.3389/fpubh.2014.00115; "The Biological and Toxin Weapon Trends Symposium."

[5] Iris Hunger, *et al.*, "The Future of Biothreat Governance," in *Biological Threats in the 21st Century*, ed. Filippa Lentzos (London: Imperial College Press, forthcoming); Gigi Kwik Gronvall, "The Threat of Misuse," in *Biological Threats in the 21st Century*; Lentzos, "The Risk of Bioweapons Use"; Jefferson, "Synthetic Biology and Biosecurity."

[6] Lentzos, *Biological Threats in the 21st Century*.

[7] Hunger, "The Future of Biothreat Governance"; Kwik Gronvall, "The Threat of Misuse"; Lentzos, "The Risk of Bioweapons Use."

While the use of biology will not have military utility in all contemporary conflicts, the possibility that it might have military utility in a small subset of conflicts, along with the erosion of technological barriers to acquire and use bioweapons, makes it imperative that the bioweapons threat from states is dedicated a greater part of the collective vigil and that effective preventive measures are developed.

## Emerging Research Areas with High Misuse Potential

Various efforts have been made, particularly in the United States, to characterize biological research with high misuse potential.[8] Examples identified of such "dual use research of concern" include experiments that increase capacity: to manipulate the pathogenicity, virulence, host-specificity, transmissibility, resistance to drugs, or ability to overcome host immunity to pathogens; to synthesize pathogens and toxins without cultivation of microorganisms or using other natural sources; to identify new mechanisms to disrupt the healthy functioning of humans, animals and plants; and to develop novel means of delivering biological agents and toxins. Early high-profile experiments that raised concern aimed to make mousepox more deadly, synthesize poliovirus from scratch and reconstruct the extinct 1918 flu virus.[9] More recently, entire fields of biological research have raised concern. These include potentially pandemic pathogens, synthetic biology and neurobiology.

### *Potentially Pandemic Pathogens*

The security community's attention was drawn to virology in 2011 when it transpired that two leading influenza laboratories, under the leadership of Ron Fouchier and Yoshihiro Kawaoka, had conducted experiments to determine whether H5N1 avian influenza, or "bird flu," could become readily transmissible between mammals and still remain highly virulent. H5N1 does not spread easily from human to human, but it kills more than 50 percent of people infected.

[8] For example: National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press, 2004); National Science Advisory Board for Biosecurity, *Proposed Framework for the Oversight of Dual-Use Life Sciences Research* (Washington: NSABB, 2007); *US Government Policy for Oversight of Life Sciences Dual Use Research of Concern* (March 2012); and *US Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern* (September 2014), available at http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/dual-use-research-concern.

[9] Ronald J. Jackson, *et al.*, "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75 (2001): 1205–1210; Eckard Wimmer, "The Test-tube Synthesis of a Chemical Called Poliovirus. The Simple Synthesis of a Virus Has Far-reaching Societal Implications," *The European Molecular Biology Organization Reports – Special Issue* 7 (2006): S3–S9; Terrence M. Tumpey, *et al.*, "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus," *Science* 310 (2005): 77–80.

Fouchier and Kawaoka were concerned that H5N1 could become readily transmissible between mammals and still remain highly virulent, and the virologists were worried that governments were not taking the threat seriously enough. In the summer of 2011, both groups passed H5N1 among ferrets as an animal model and discovered that a mutated H5N1 virus that was air transmissible could indeed emerge. In other words, what they had developed in their labs was a novel, more contagious strain of the bird flu virus that could spread to humans and other mammals.

Kathleen Vogel describes the unfolding story in some detail.[10] In essence, Fouchier submitted his paper to the prestigious journal *Science*; Kawaoka favored *Nature.* In September 2011, Fouchier revealed his findings at a scientific meeting in Malta: his mutated virus was airborne and as efficiently transmitted as the seasonal flu virus. In public, he commented that "[t]his is a very dangerous virus."[11] His funder, the National Institutes of Health (NIH), grew concerned about the security implications if the results were published: could bioterrorists (or indeed national militaries) adopt similar "gain-of-function" techniques to increase the pathogenicity and transmissibility of viruses? The NIH asked the US National Science Advisory Board on Biosecurity (NSABB), the government advisory body on dual use life science research oversight, to review both papers. By the end of November 2011, NSABB recommended that the papers' general conclusions highlighting the novel outcome be published, but that the manuscripts not include a methods section with details of how to carry out the experiments.[12] This was the first time NSABB had recommended restrictions on scientific publications in the life sciences.

The safety and security implications of the experiment garnered a great deal of media coverage. *The New York Times* ran an editorial with the unambiguous headline, "An Engineered Doomsday," arguing that the modified flu virus could kill tens or hundreds of millions of people if it escaped the lab or was stolen. Proponents of gain-of-function research, on the other hand, argued that such studies help understand influenza transmission and can assist public health researchers in detecting an impending flu pandemic and preparing vaccines.

[10] Kathleen M. Vogel, "Expert Knowledge in Intelligence Assessments: Bird Flu and Bioterrorism," *International Security* 38 (Winter 2013–2014): 39–71.

[11] Quoted in Katherine Harmon, "What Really Happened in Malta This September When Contagious Bird Flu Was First Announced," *Scientific American* (blog), 30 September 2011, http://blogs.scientificamerican.com/observations/what-really-happened-in-malta-this-september-when-contagious-bird-flu-was-first-announced/. In late September, an article in *New Scientist*, a weekly science and technology news magazine, first reported that Fouchier's modified H5N1 virus was lethal to the ferrets in the experiments – see Debora MacKenzie, "Five Easy Mutations to Make Bird Flu a Lethal Pandemic," *New Scientist*, 26 September 2011, www.newscientist.com/article/mg21128314-600-five-easy-mutations-to-make-bird-flu-a-lethal-pandemic/.

[12] U.S. Department of Health and Human Services, "Press Statement on the NSABB Review of H5N1 Research," *NIH News*, 20 December 2011, http://www.nih.gov/news/health/dec2011/od-20.htm.

In January 2012, a prominent group of virologists wrote to NSABB to reconsider. NSABB published an explanation and defense in both *Nature* and *Science*. The primary reason for the unprecedented redaction was that "publishing these experiments in detail would provide information to some person, organization, or government that would help them develop similar mammal-adapted influenza A/H5N1 viruses for harmful purposes." By mid-February 2012, the World Health Organization (WHO) convened a technical consultation on the Fouchier and Kawaoka experiments.[13] Both scientists attended and presented new data related to the manuscripts. The WHO meeting agreed a temporary moratorium was needed to address public concerns. Fouchier and Kawaoka were to revise their manuscripts with new details and submit them to NSABB for a second security review.

Fouchier backtracked. He then stated that his group's mutated virus was not lethal when inhaled by ferrets and would not spread "like wildfire" through the air; rather, transmission would not be easy. He also said that most of the ferrets that had contracted the virus via aerosol transmission had hardly become sick, and none had died. He clarified, however, that the mutated virus did cause disease when injected in very high concentrations into the lower respiratory tract of ferrets.

In the end, NSABB recommended publication of Kawaoka's revised paper in full, but some board members continued to have concerns about Fouchier's paper. They felt it was "immediately and directly enabling" for terrorism (and biological warfare) and a "pretty complete cookbook" for causing harm. By May 2012 Kawaoka's paper was published in *Nature*. Fouchier's paper followed suit and was published in *Science* in June 2012.

Following the voluntary moratorium, work resumed on potentially pandemic pathogens in 2013, with scientists in multiple labs adding new properties to biological agents and creating modified variants of viruses that do not currently exist in nature. Within a short space of time, however, new papers on human-made H5N1 and other dangerous flu strains rekindled concerns about potentially pandemic pathogens created in the lab – in part because a series of lab accidents and breaches at the NIH and Centers for Disease Control and Prevention (CDC) raised questions about safety at high-containment labs. On 17 October 2014, the US government stepped in, imposing a federal funding pause on potentially pandemic pathogen experiments and announcing an extended deliberative process, which is still on-going.[14]

[13] World Health Organization, "Technical Consultation on H5N1 Research Issues – Consensus Points," 16–17 February 2012, http://www.who.int/influenza/human_animal_interface/consensus_points/en/index.html; and World Health Organization, "Public Health, Influenza Experts Agree H5N1 Research Critical but Extend Delay," 17 February 2012, www.who.int/mediacentre/news/releases/2012/h5n1_research_20120217/en/index.html.

[14] "U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS, and SARS

## Synthetic Biology

Many have viewed the controversy around potentially pandemic pathogens as a test case of what is to come when the still-emerging field of "synthetic biology" begins to mature. Synthetic biology aims to engineer biology, or "to design and engineer biologically based parts, novel devices and systems, as well as redesigning existing, natural biological systems."[15] The aspirations and pace of advance in synthetic biology have raised a number of security concerns. Some of these are legitimate, others less so.[16]

One of the main trepidations raised in the political and security discourse is that synthetic biology is making it easier to create dangerous pathogens from scratch. The claim is that well-characterized biological parts can be easily obtained from open-source online registries and then assembled, by people with no specialist training outside professional scientific institutions, into genetic circuits, devices and systems that will reliably perform desired functions in live organisms. This narrative rests on misleading assumptions about synthetic biology.

The narrative does not reflect the situation facing people with no specialist training who work outside professional scientific institutions, nor does it even reflect current realities in academic or commercial science laboratories: academic and commercial researchers are still struggling with every stage of the standardization and mechanization process. More than a decade in, the translation of proof-of-concept designs into real-world applications is still a major challenge. As recently noted in the scientific literature surveying progress in synthetic biology, "The synthetic part is easy, it's the biology part that's confounding."[17] However, even if the engineering approaches offered by synthetic biology make processes more systematic and more reproducible, skills do not become irrelevant, and all aspects of the work do not become easier. Further, importantly, "easier" does not mean "easy." Aeronautical engineering provides a useful analogy: planes are built from a large number of well-characterized parts in a systematic way, but this does not mean that any member of the general public can build a plane, make it fly and use it for commercial transportation. Thus, advances in synthetic biology do not make it easier for just anybody to engineer biological systems, including dangerous ones.

Viruses," 17 October 2014, http://www.phe.gov/s3/dualuse/Documents/gain-of-function.pdf (accessed 20 January 2016).

[15] The Royal Academy of Engineering, *Synthetic Biology: Scope, Applications and Implications* (London: The Royal Academy of Engineering, 2009).

[16] Filippa Lentzos, Catherine Jefferson, and Claire Marris, "The Myths (and Realities) of Synthetic Bioweapons," *The Bulletin of Atomic Scientists*, 18 September 2014, http://thebulletin.org/myths-and-realities-synthetic-bioweapons7626; Jefferson, *et al.*, "Synthetic Biology and Biosecurity."

[17] Timothy S. Gardner, *et al.*, "Synthetic Biology: From Hype to Impact," *Trends in Biotechnology* 31:3 (2013): 123–125, quoted in *Nature Reviews Microbiology* 12:5 (2014): 309.

This leads to a second concern raised in the political and security discourse: that synthetic biology is breaking down the expert and non-expert boundary. In other words, the growth of a do-it-yourself biology (DIY bio) community, along with DNA synthesis becoming cheaper and easily outsourced, could make it easier for terrorists to obtain the basic materials to create biological threat agents. However, the link between synthetic biology and DIY bio, and the level of sophistication of the experiments typically being performed, is grossly overstated. DIY biologists typically comprise a wide range of participants of varying levels of expertise, ranging from complete novices with no prior background in biology to trained scientists who conduct experiments in their own time. Some DIY biologists work in home laboratories assembled from everyday household tools and second-hand laboratory equipment purchased online; the majority conduct their experiments in community labs or "hackerspaces." Studies of scientific practice in community labs demonstrate the challenges that amateur biologists face while trying to successfully conduct even rudimentary biological experiments. These amateurs particularly lack access to the shared knowledge available to institutional researchers, highlighting the importance of local, specialized knowledge and enculturation in laboratory practices.

DNA synthesis is one of the key enabling technologies of synthetic biology. There are now a number of commercial companies that provide DNA synthesis services, so the process can be outsourced: a client can order a DNA sequence online and receive the synthesized DNA material by post within days or weeks. The price charged by these companies has greatly reduced over the last 20 years and the service is now within reach of a broad range of actors. This has led to routine statements suggesting that it is now cheap and easy to obtain a synthesized version of any desired DNA sequence.

There are, however, several challenges that need to be taken into account when assessing the potential for misuse that inexpensive DNA sequencing might enable. First, simply ordering online the full-length genome sequence of a small virus (or those of larger bacteria) is not currently possible. The alternative, ordering short DNA sequences and assembling them into a genome, requires specialist expertise, experience and equipment available in academic laboratories, but not easily accessible to an amateur working from home. As noted by NSABB, while the "technology for synthesizing DNA is readily accessible, straightforward and a fundamental tool used in current biological research … the science of constructing and expressing viruses in the laboratory is more complex and somewhat of an art. It is the laboratory procedures downstream from the actual synthesis of DNA that are the limiting steps in recovering viruses from genetic material."[18] Again, it is the biology and not the synthetic part that is complicated, and DNA synthesis requires extensive training in basic molecular-biology techniques, such as ligation and cloning, including

[18] National Science Advisory Board for Biosecurity (NSABB), *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents* (Bethesda, MD: National Institutes of Health, 2006), 4.

hands-on experience that is not "reducible to recipes, equipment, and infrastructure."[19]

A third frequently voiced concern is that synthetic biology may enable radically new pathogens to be designed and synthetic biology could be used to enhance the virulence or increase the transmissibility of known pathogens, creating novel threat agents. Again, it is not that simple. The mousepox and bird flu (H5N1) experiments are frequently cited to demonstrate how dangerous new pathogens could be created. However, assessments of this threat tend to overlook a salient fact: in both these experiments, the researchers did not actually design the pathogens. With respect to H5N1, researchers had indeed been trying to design an air-transmissible virus variant for some time, without success. The ferret experiment was set up as an alternative approach, to see whether natural mutations could generate an air-transmissible variant. The researchers had no influence on the specific mutations induced. In the mousepox experiment, researchers inserted the gene for interleukin-4 into the mousepox virus to induce infertility in mice and serve as an infectious contraceptive for pest control. The result—that the altered virus was lethal to mice—was unanticipated by the researchers; namely, it was not designed.

Moreover, some of the lessons that came out of the extensive Soviet program to weaponize biological agents involve the trade-offs between improving characteristics that are desired in the context of a bioweapons program, such as virulence, and diminishing other equally desired characteristics, such as transmissibility or stability. Pleiotropic effects—that is, when a single gene affects more than one characteristic and genetic instability—are common in microorganisms. While it is too simple to say that increased transmissibility will always be associated with reduced virulence, this is often the case for strains produced in laboratories. As other commentators have noted,

> To create … an artificial pathogen, a capable synthetic biologist would need to assemble complexes of genes that, working in union, enable a microbe to infect a human host and cause illness and death. Designing the organism to be contagious, or capable of spreading from person to person, would be even more difficult. A synthetic pathogen would also have to be equipped with mechanisms to block the immunological defenses of the host, characteristics that natural pathogens have acquired over eons of evolution. Given these daunting technical obstacles, the threat of a synthetic 'super-pathogen' appears exaggerated, at least for the foreseeable future.[20]

In sum, it is likely, in the near future, that synthetic biology will make it possible to create dangerous viruses from scratch. However, while synthetic biology is "deskilling" the science, it is not doing this to the extent that people with

[19] Kathleen Vogel, "Bioweapons Proliferation: Where Science Studies and Public Policy Collide," *Social Studies of Science* 36:5 (2006): 676.

[20] Jonathan B. Tucker and Raymond A. Zilinskas, "The Promise and Perils of Synthetic Biology," *The New Atlantis* 25 (2006): 38.

no specialist training operating outside professional scientific institutions can assemble biological parts into circuits, devices and systems that will reliably perform desired functions in live organisms, and even professionals will have a hard time creating radically new pathogens or synthetic "super-pathogens." The most significant misuse risks from synthetic biology do not, therefore, arise from bioterrorists, but from professional and well-resourced institutions like national militaries.[21]

The most recent figures available on US trends in synthetic biology research funding indicate that two thirds of the $ 200 million invested in 2014 came from the Department of Defense (DoD) or its research agency DARPA.[22] From an international security perspective, the extensive influx of military funding can be perceived as threatening to analysts in other countries following these developments. The DoD declared just over $655 million on national biodefense research in 2014; synthetic biology research would appear, then, to make up about a fifth of the biodefense budget.[23]

Funding in other countries is also increasing rapidly. In 2014, the UK and European Commission investment in synthetic biology made up nearly 30 percent of total Euro-American synthetic biology funding.[24] Some of this European funding is also defense-related. In the UK, for instance, which spends twice as much as the European Commission on synthetic biology, the field is one of five emerging technologies identified by the Ministry of Defence as having the most potential for national security. It is crucial that military research in this field remain as transparent as possible to ensure there is confidence that the fine line between permitted defense work and non-permitted offensive work does not become muddled.

## Neurobiology

Neurobiology is another emerging area with high misuse potential.[25] Military interest in neurobiology mainly relates to enhancement, involving efforts to

[21] Jefferson, *et al.*, "Synthetic Biology and Biosecurity."

[22] "US Trends in Synthetic Biology Research Funding" (Washington DC: Wilson Center, 2015), available at http://www.synbioproject.org/site/assets/files/1386/final_web_print_sept2015.pdf (accessed 20 January 2016).

[23] US Department of State, *Confidence-Building Measure Return Covering 2014: Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, submitted to the United Nations on 15 April 2015, available at www.unog.ch/80256EDD006B8954/(httpAssets)/4631533639F1D34AC1257E380046511B/$file/BWC_CBM_2015_USA_Public.pdf (accessed 20 January 2016).

[24] *US Trends in Synthetic Biology.*

[25] National Research Council, *Emerging Cognitive Neuroscience and Related Technologies* (Washington, DC: National Academies Press, 2008); The Royal Society, *Neuroscience, Conflict and Security* (London: The Royal Society, 2012), http://royalsociety.org/policy/projects/brain-waves/society-policy/ (accessed 20 January 2016); Tim Requarth, "This is Your Brain. This Is Your Brain as a Weapon," *Foreign Policy*, 14 September 2015, http://foreignpolicy.com/2015/09/14/this-is-your-brain-this-is-your-

improve the operational performance of national forces, and to degradation, involving efforts to diminish the performance of the enemy.

There are various ways neurobiology might confer performance advantages in a military context.[26] One of these is through the use of neuropharmacological agents to enhance cognitive functions like perception, attention, learning, memory, language, thinking, planning and decision-making. There has been significant military interest in cognitive enhancement. Modafinil—discovered by French scientists in the 1970s and since licensed as a common treatment for narcolepsy, but which has also been shown to enhance working memory and executive functioning in non-sleep-deprived individuals—is thought to have been used by the French army in Iraq in the early 1990s to combat fatigue and by the US Air Force in 2003 to improve alertness and concentration during long flights.[27] Military interest in sustaining and enhancing brain function and performance continues, demonstrated by the large number of DARPA projects devoted to this goal.[28] Neurobiology has also been identified by the UK Ministry of Defence as an important and rapidly developing field with potential relevance to defense and security.[29]

Degrading enemy performance through neurobiology has focused particularly on the development of incapacitating biochemical agents, or so-called non-lethal weapons. Incapacitants generally target the central nervous system to reduce alertness and, as the dose increases, produce sedation, sleep, anesthesia and death; these are distinct from riot control agents, such as tear gas, which cause local irritation to eyes, skin and the respiratory tract, and have long been used by police forces around the world.

Despite international agreement on the Chemical Weapons Convention (CWC) in 1993, there are indications of continued interest in incapacitating biochemicals among a number of states. The CWC bans the use of all toxic chemicals as weapons in war, but it does not prevent states from using toxic chemicals such as "tear gasses" for law enforcement and domestic riot control. Though the range of permitted toxic chemicals is restricted by types and quantities consistent with law enforcement purposes, some states have interpreted this law enforcement exemption to extend to incapacitating chemical agents.

Concern over state interest in incapacitants was heightened following a case of actual use by the Russian Federation in October 2002.[30] A group of armed Chechen separatists raided the Dubrovka Theater in Moscow and took approximately 800 hostages. They demanded the withdrawal of Russian troops from

brain-as-a-weapon-darpa-dual-use-neuroscience/ (accessed 20 January 2016).

[26] Royal Society, *Neuroscience, Conflict and Security*, Chapter 4 "Performance Enhancement."

[27] Ibid.

[28] Ibid., 6 and 35–36.

[29] Ibid.

[30] Neal Davison, *"Non-Lethal" Weapons* (London: Palgrave Macmillan, 2009), 12–13.

Chechnya and threatened to kill the hostages if their demand was not met. Russian Special Forces disseminated an incapacitating chemical agent—reportedly a mixture of derivatives of the synthetic opiate fentanyl—through the ventilation system of the theater, rendering both the hostages and the hostage-takers unconscious. Shortly afterwards, the troops stormed in, killing all of the hostage-takers and bringing the siege to an end. 129 of the hostages died from use of the incapacitant and many others suffered serious and long-term injury. The refusal of the Russian Special Forces to disclose the identity of the incapacitating agent at the time of the siege prevented emergency medical personnel from responding effectively. There are also indications that the Russian Federation has continued research into incapacitating biochemical agents following this event.[31] The US, too, has had a long-standing interest in incapacitating biochemical agents.[32]

As with synthetic biology, current investments in the field of neurobiology are considerable. The European Commission-funded Human Brain Project, established in 2013, has an estimated € 1 190 million price tag over ten years.[33] The US equivalent, the BRAIN Initiative, was also launched in 2013, as a public-private partnership with about $ 100 million in the President's Fiscal Year 2014 Budget.[34] Approximately half of the US funding comes from the DoD and DARPA.[35]

Developments in anesthetics and neuropharmacological drug research, coupled with developments in drug delivery, are making precise manipulation of neurological function increasingly feasible and there are concerns about the risk incapacitants pose to the international ban on chemical weapons. Particularly relevant to the BWC are bioregulators and their synthetic derivatives.[36] Bioregulators are specialized chemicals that carry messages from the brain to the rest of the body, between neurons or within cells, and modulate the function of the target cell or organ. They are naturally occurring biochemical compounds, such as hormones, neurotransmitters or signaling factors that control vital homeostatic systems like temperature, sleep, blood pressure, heart rate and immune response. However, while they occur naturally in the body at low concentrations, they can be extremely toxic at higher concentrations or if the molecular structure is changed. While many bioregulators tend to be unstable in aerosolized form and are rapidly broken down by enzymes in the body, engineered variants could be synthetized, and considerable developments have

[31] Royal Society, *Neuroscience, Conflict and Security*.

[32] Ibid.

[33] *The Human Brain Project: A Report to the European Commission* (Lausanne: The HBP-PS Consortium, 2012), https://www.humanbrainproject.eu/documents/10180/17648/TheHBPReport_LR.pdf (accessed 20 January 2016).

[34] The White House, "Fact Sheet: BRAIN Initiative," 2 April 2013, www.whitehouse.gov/the-press-office/2013/04/02/fact-sheet-brain-initiative (accessed 20 January 2016).

[35] Ibid.

[36] Royal Society, *Neuroscience, Conflict and Security*, 49–50.

taken place in the *in vitro* synthesis of bioregulators for pharmaceutical purposes. Aerosol technology is also advancing rapidly and is already in use to deliver effective inhaled drug therapy for the treatment of disease.[37] Propellant metered-dose inhalers, dry powder inhalers and nebulizers are used to deliver drugs directly to the lungs, promoting rapid absorption into the blood. Advances in research into inhalation based methods of drug and vaccine delivery may also offer potential applications in the delivery of bioregulators. With advances in neurobiology, it may eventually become possible to develop modified bioregulators that can be disseminated over large crowds of people and that will cross the blood-brain barrier to induce states of sleep, confusion, placidity, fear, addiction or aggression.[38]

The European Human Brain Project has made an explicit commitment not to take funds from the military or to develop applications with military objectives.[39] It also has an "ethics and society" component that aims "to explore the project's social, ethical and philosophical implications, promote engagement with decision-makers and the general public, foster responsible research and innovation by raising social and ethical awareness among projects partners and ensure that the project complies with relevant legal and ethical norms."[40] To date, there are no such equivalent efforts underway in the American program.

## Fostering Responsible Science

Pandemic pathogens, synthetic biology and neurobiology are three fields of bioscience that have particularly high potential for misuse. There are, of course, also other areas of research with misuse potential. While the BWC and Geneva Protocol provide a legal and normative frame, continued efforts are required in multilateral, national and scientific spheres to strengthen the red lines about the misuse of biology. Crucial areas to strengthen are (1) the international legal framework regulating biological weapons, (2) the BWC science and technology review procedure and (3) norms of transparency and public accountability.

### *1. Strengthen the international legal framework regulating biological weapons*

Article IV of the BWC commits Member States to both prohibit and prevent biological weapons activities. This means they are not only obliged to respond to prohibited activities but also to stop them from happening. An important mechanism of enforcement is criminalization.

[37] Ibid., 50.

[38] Ibid.

[39] https://www.humanbrainproject.eu/documents/10180/538356/HBP_FPA_PRINT_29-07-14.pdf (accessed 20 January 2016).

[40] https://www.humanbrainproject.eu/discover/ethics (accessed 20 January 2016).

Criminalization at the international level, as an international crime or war crime, provides the strongest and most effective measure for individual liability for violations of international law. Neither weaponization of biology nor use of biological weapons has been comprehensively criminalized in the Rome Statute of the International Criminal Court (ICC).[41] The use of "poison or poisoned weapons," a prohibition first codified in 1899, is stipulated as a war crime.[42] Another paragraph is derived from the 1925 Geneva Protocol, making the use of asphyxiating, poisonous or other gases and all "analogous liquids, materials or devices" a war crime. The provision notably does not refer to the use of bacteriological weapons, which is prohibited in the Geneva Protocol, and makes no further reference to either chemical or biological weapons. Some commentators maintain that biological weapons are nevertheless included – relying on the premise that the term "poisoned weapon" was the first prohibition of both chemical and biological weapons.[43] However, most commentators conclude that biological weapons are not included in the Rome Statute.[44] The absence of a provision explicitly making the use of biological weapons a war crime under the Rome Statute is a striking gap in the international legal regulation of biological weapons and must swiftly be rectified.

### *2. Strengthen the BWC science and technology review procedure*

Developments in science and technology play a fundamental role in the continued relevance of the BWC. These developments are, however, highly technical in nature, and the process through which BWC Member States identify science and technology developments and assess their implications must reflect this. Whilst the current intersessional work program of the treaty provides limited time and space to comprehensively deal with science and technology challenges, addressing these issues primarily within the policy work of the treaty further complicates efforts. More time and a different environment are needed.

A dedicated technical body such as an open-ended working group with its chair and vice chairs appointed for several years at a time would help insulate technical discussions from policy considerations. The group should be expert-

[41] Use of biological weapons will in many cases be covered by *other* provisions, such as Rome Statute of the International Criminal Court, article 8(2)b) (xx), prohibiting methods and materials of warfare that are of a nature to cause superfluous injury or unnecessary suffering, or are inherently indiscriminate, if and when an annex has been agreed to the provision. See Filippa Lentzos and Cecilie Hellestveit, "The Categorical Ban on Bioweapons: Challenged by Synthetic Biology?" in *High-Tech War and International Law*, ed. Guglielmo Verdirame, *et. al.* (forthcoming).

[42] Rome Statute of the International Criminal Court, Article (2)(b)(xvii).

[43] Michael Cottier,"War Crimes: Article 5," in *Commentary on the Rome Statute of the International Criminal Court, Observers' Notes, Article by Article*, ed. Otto Triffterer, 2nd edition (Oxford: Hart Publishing, 2008), 413.

[44] Markus Wagner, "The ICC and its Jurisdiction – Myths, Misperceptions and Realities," in *Max Planck Yearbook of United Nations Law*, vol. 7, ed. Armin von Bogdandy and Rüdiger Wolfrum (Boston: Brill, 2004), 460.

led and inclusive, open to all signatories and to academies of science and other relevant organizations that could help in making these collective judgments. This would help ensure that discussions remain technical, that the conclusions reached are factual and that any recommendations made have a sound scientific basis. Clear topics for consideration include potentially pandemic pathogens, synthetic biology and neurobiology, as well as the increasing convergence of biology with other fields, particularly with chemistry, and the implications of this for arms control and international law.

The group should meet separately from the Meeting of Experts in a restructured intersessional process and feed its recommendations to the member states directly. It needs to be adequately resourced and a scientific secretary should be appointed to provide continuous professional support. It should have a mandate as an organ of the Convention carrying forward the science and technology review function envisaged from the start in Article XII, but on a more systematic basis.

### *3. Strengthen norms of transparency and public accountability*

The life science community plays a crucial role in sustaining biological disarmament and non-proliferation. The health of the BWC rests on individual life scientists and the systems and safeguards where they work, on an awareness of dual-use problems and structures to encourage responsible behavior, on biosafety and biosecurity and all the elements of good practice for those engaged in relevant science and technology. Key to this is education. Not education in the sense of implanting facts and knowledge and instructing people in what to think, but education in the sense of eliciting understanding and teaching people how to think for themselves. It is about equipping life scientists with sensitivity to the risk that the knowledge gained from the experiments and research they carry out can be misused.

Education, however, is not an end in itself; in this case, it would rather provide an avenue by which to affect behavior. The ultimate aim is that life scientists behave responsibly, as well as provide a layer of oversight about the work carried out in their laboratories and in their specialized fields. The rapid pace and nature of change in the life sciences today means that anyone other than practicing life scientists is hard-pressed to have the sort of current, technical expertise required to provide adequate oversight. Education and awareness-raising efforts must, therefore, go hand-in-hand with the development of supportive structures and professional practices for flagging any suspect activities or worrying advances in the field.

Although life scientists may feel autonomous in their work, most remain susceptible to larger institutional and political pressures. Whether in academic medical centers, pharmaceutical companies or government facilities, they work in settings where norms, professional responsibilities and missions are bureaucratically defined. However, these scientific communities also respond to national norms concerning transparency and public accountability. BWC signatories must therefore view national implementation of the treaty within states, and transparency and compliance assurance mechanisms between states, as vehicles for promoting norms of transparency and public accountability and for fostering responsible science.

## About the author

Filippa Lentzos, PhD, is a senior research fellow in the Department of Global Health & Social Medicine at King's College London. Her research focuses on political, legal and security aspects of emerging technologies in the life sciences. Forthcoming titles include *Biological Threats in the 21$^{st}$ Century* (Imperial College Press, 2016) and *Synthetic Biology & Bioweapons* (World Scientific, 2016).
E-mail: filippa.lentzos@kcl.ac.uk.

*Connections: The Quarterly Journal*
ISSN 1812-1098, e-ISSN 1812-2973

Bastian Giegerich, *Connections QJ* 15, no. 2 (2016): 65-72
http://dx.doi.org/10.11610/Connections.15.2.05

Research Article

# Hybrid Warfare and the Changing Character of Conflict

*Bastian Giegerich*

*International Institute for Strategic Studies (IISS), London, http://www.iiss.org*

**Abstract**: The idea that international conflict might be seeing more hybrid warfare and hybrid threats has animated debate among security and defense establishments in the run-up to NATO's 2016 Warsaw Summit. While the Alliance has located the issue of hybrid war in the specific context of the Russia/Ukraine crisis and in 2014 triggered efforts to prepare NATO to effectively meet hybrid warfare threats, the scope of the challenge is much wider and the core dynamics are often located outside of the military realm. The article reviews the recent conceptual debates about hybrid warfare, suggesting that hybrid conflicts defy our attempts to press them into known categories and locate them clearly on a spectrum of war and peace. NATO Member States will have to invest in resilience and conventional deterrence to counter hybrid threats.

**Keywords**: hybrid threats; conflict; resilience; deterrence; strategy.

From "little green men" in Crimea to "little blue men" in the South China Sea, the idea that international conflict might be seeing more hybrid warfare and hybrid threats has animated debate among security and defense establishments in NATO and beyond.[1] In fact, the term hybrid warfare has become a bit of a staple of Europe's security policy vocabulary. NATO and the EU are working on strategy papers aimed at strengthening defensive capabilities and preventing hybrid attacks. National governments drafting security and defense review documents make frequent reference to the need to address hybrid threats. Journalists have adopted the term "hybrid war" as a shorthand for Russian tac-

[1] Both terms refer to unbadged personnel, see: Vitaly Shevchenko, "'Little Green Men' or 'Russian invaders'?" *BBC News*, 11 March 2014; Christopher Cavas, "China's 'Little Blue Men' Take Navy's Place in Disputes," *Defense News*, 2 November 2015.

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

tics in Ukraine, apparently with the assumption that readers already know what this means.

NATO's Wales Summit Declaration from 5 September 2014 says Alliance leaders "will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces."[2]

While the Wales declaration put the issue of hybrid war in the specific context of the Russia/Ukraine crisis and triggered efforts to prepare NATO to effectively meet such threats, the scope of the challenge is much wider and the core dynamics are often located outside the military realm. Earlier work conducted at NATO Allied Command Transformation under the label "Countering Hybrid Threats" acknowledges as much, but it seems as if the insights generated at the time were not systematically pursued until Russia's illegal annexation of Crimea served as a stark reminder.[3]

## Why Should We Care?

With a view to the conflict in Ukraine, analysts come to different assessments. Anton Dengg and Michael Schurian argue the Ukraine conflict suggests employing hybrid means to project power might be an important trend that could shape the character of threats to come.[4] The British National Security Strategy and its supporting Strategic Defence and Security Review, published at the end of November 2015, state that "the illegal annexation of Crimea in 2014 and continuing support for separatists in eastern Ukraine through the use of deniable, hybrid tactics and media manipulation have shown Russia's willingness to undermine wider international standards of cooperation in order to secure its perceived interest."[5] These strategic documents treat hybrid threats both as tier one challenges, which might affect the UK directly, and as tier two threats, which would start as a hybrid attack on an ally. Diego Ruiz Palmer summarizes Russia's aims as achieving "politically decisive outcomes with, if possible, no or

[2] NATO, "Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm (accessed 11 December 2015).

[3] For a summary of the ACT work, see Michael Miklaucic, "NATO Countering the Hybrid Threat," 23 September 2011, http://www.act.nato.int/nato-countering-the-hybrid-threat (accessed 11 December 2015).

[4] Anton Dengg and Michael Schurian, Zum Begriff der Hybriden Bedrohungen, in *Vernetzte Unsicherheit – Hybride Bedrohungen im 21. Jahrhundert*, ed. A. Dengg and M. Schurian (Vienna: Landesverteidigungsakademie, 2015), 23–75.

[5] HM Government, National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom, November 2015, Cm 9161, at 18.

only a limited and overt use of military force, while being prepared to act militarily, with devastating effect at the operational level… aim at attaining a decisive political advantage *short of war*."[6] The main takeaway is that much of the activity related to hybrid conflict will take place beneath the threshold that most Western observers would consider armed conflict, much less war.

Samuel Charap at the International Institute for Strategic Studies suggests that Russia's approach would not travel well beyond the specific circumstances of the conflict in Ukraine. Charap maintains Russia does not have "a hybrid-war doctrine that could be effectively deployed against NATO" and goes on to warn talking up the issue of hybrid warfare poses a danger in itself: "Russian strategists believe that the US is willing to risk conducting a limited, hybrid operation in Russia … just as NATO strategists believe Russia is willing to risk the same on the territory of [NATO]."[7] Can Kasapoglu, in a rather nuanced analysis, points out that NATO might not be facing a new Russian military strategy, but the Alliance should realize that "new military thinking that brings about shifts at strategic, operational, and tactical levels along with doctrinal order of battle and military strategic culture" has emerged in Russia around the concept of non-linear warfare.[8] Lawrence Freedman offers yet another perspective, submitting that Russia may well have conducted hybrid warfare in Ukraine, but was actually not very successful and the advantages offered to the attacker by hybrid means are exaggerated.[9]

Aside from the question of whether Russian behavior in Ukraine is a model for hybrid warfare and, if so, how far can it be generalized and was successful, another core debate rages around the issue of the appropriateness of the label itself. To some observers the current preoccupation with hybrid warfare is a fad at best, and represents intellectual laziness at worst. Proponents of the former view would insist that we are not actually witnessing anything new, but merely a modern-day interpretation of the time-honored combination of conventional and unconventional approaches. Supporters of the latter view might argue that hybrid warfare has become a convenient label to file away all the issues we currently do not understand about the changing character of conflict. Overall, however, while its nature and importance might well be contested, ignoring the evolution of a hybrid approach to conflict would come at the Alliance's peril.

Frank Hoffman's writing is a good analytical starting point to clarify the concept, not least because Hoffman was among the writers who coined the term in its current incarnation. He stresses that hybrid threats amount to much more

[6] Diego A. Ruiz Palmer, "Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons," Research Paper No. 120 (NATO Defense College, October 2015), 2.

[7] Samuel Charap, "The Ghost of Hybrid War," *Survival* 57:6 (2015): 53, 57.

[8] Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," Research Paper No. 121 (NATO Defense College, November 2015), 11.

[9] Lawrence Freedman, "Ukraine and the Art of Limited War," *Survival* 56:6 (2014): 7–38.

than simple combinations of a variety of actors, tactics and approaches. Hybrid challengers fuse different modes of conflict and it is that new synthesis that emerges that is difficult to deal with, because it confounds Western binary conceptions of peace and war, of military and non-military means, and of conventional and irregular approaches.[10] Commenting recently on the matter, Hoffman said Western actors "think of things in black-and-white terms" and still need to improve significantly at understanding conflict in the spaces in between, in the grey areas.[11] Given that a fusion of conflict patterns, which had previously been seen as unconnected, is the core of hybrid threats, it logically follows that hybrid threats and hybrid warfare will come in many guises – this challenge will continue to evolve.

One does not have to subscribe to a whole new hybrid paradigm to acknowledge that hybrid warfare and hybrid threats currently do affect European security directly and also can serve as a useful construct to think through the capabilities to prevent and counter certain contemporary challenges. In itself, the combination of regular and irregular forces in one theater of operations is of course quite a conventional strategy.[12] What is new, however, is the immediate relevance to Europe's security today. Hybrid actors in the East and South are directly threatening European security interests, and even appear to be calling the entire Euro-Atlantic security order into question. Vladimir Putin's great power ambitions are incompatible with the principles and value structure of European security institutions. Yet with regard to the Russian government, the established methods of international relations, including their military dimensions, should still be effective. On the other hand, the caliphate of Abu Bakr al-Baghdadi, the barbarity and nihilistic contempt for humanity of the so-called Islamic State (IS), makes a negotiated solution with this actor seem unlikely, if not plain absurd. Both are hybrid challengers.

Hybrid wars have therefore reached Europe from two directions, and in very different form. In the East is a state actor, Russia under Putin, who deliberately uses non-state means, and in the South is a non-state actor, Islamic State (IS), whose leaders are attempting to establish structures that are at least similar to those of a state, and who also have access to means of violence that ordinarily

[10] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), at www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (accessed 11 December 2015); James N. Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings Magazine*, 132:11 (2005), http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (accessed 11 December 2015).

[11] Quoted in Thomas Gibbons-Neff, "The 'new' type of war that finally has the Pentagon's attention," *Washington Post*, 3 July 2015, https://www.washingtonpost.com/world/national-security/the-new-type-of-war-that-finally-has-the-pentagons-attention/2015/07/03/b5e3fcda-20be-11e5-84d5-eb37ee8eaa61_story.html (accessed 11 December 2015).

[12] Max Boot, "Countering Hybrid Warfare," in *Armed Conflict Survey 2015* (Abingdon: International Institute for Strategic Studies, 2015), 11–20.

tend to be afforded to states, or more precisely to their armed forces. These enemies of Europe are hybrid entities in the sense that they are able to use all available instruments of power in a theater of operations in a coordinated way, and with at least a certain degree of central control. At the same time, they pursue the same goals that have always motivated actors in armed conflicts: gaining a psychological and physical advantage. In this struggle, hybrid warfare is no different from other forms of war.

## Implications of the Hybrid Approach to Conflict and Policy Recommendations

As has been suggested, the implications of a hybrid approach to conflict are wide-ranging and cut across concepts, material capability aspects, legal matters, and institutional innovation.[13] Hybrid conflict defies the attempt to press it into known categories. It is not simply in-between state-driven conflict and non-state-driven conflict, as the recent US military strategy suggests.[14] That particular strategic document does have the advantage, though, of thinking about conflict in terms of a continuum, rather than suggesting distinct conditions such as war and peace. Hybrid conflict takes place in the intermediate spaces, or at the seams of traditional ways of thinking.

On the response side, the key conceptual innovation has been the discovery, or perhaps the rediscovery, of resilience as the underpinning principle of security policy. Resilience in the context of national security refers to the ability of societies to manage threats and risks, to adapt to them, and to recover from them should an attack or event occur, without losing the ability to provide basic functions and services to the members of that society.[15] In short, it is the capacity to degrade gracefully under pressure and then bounce back. Resilience is foremost a matter of reducing one's own vulnerabilities. Given that doing so makes it less likely that hybrid attackers manage to achieve their intended goals, resilience also contributes to deterrence in a hybrid context by reducing the potential gains any attacker might hope to reap.

If hybrid war is the evil twin of NATO's comprehensive approach, an implication is actually that NATO will have to redouble its efforts to make the comprehensive approach more successful and in particular strengthen the links with other organizations. It is clear that even deciding on responsibilities at the national level and task-sharing between NATO, the EU, and other organizations will be anything but easy. Preventing and defending against hybrid threats will need to involve the entire government on the national and local level, the pri-

[13] Patryk Pawlak, "Understanding Hybrid Threats," European Parliamentary Research Service (EPRS), 24 June 2015.

[14] US Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015* (Washington, DC: DOD, 2015), 4.

[15] Oliver Tamminga, "Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie," *SWP-Aktuell* 92 (2015): 3.

vate sector, and arguably society as a whole. The synergies of the networked approach, so straightforward in theory, are hard to achieve in practice. There is no single responsibility for defense against hybrid threats and therefore no obvious center of decision-making. The spectrum is wide, and systematically checking which organization and body would be in charge of each element of a response to a hybrid attack will produce a picture that makes it only too clear that at the national level, and international level, the available instruments are insufficiently interconnected. As Christian Mölling has argued, a hybrid security policy is the appropriate answer to hybrid threats in order to meet "adversaries in the non-military arena to prevent an escalation toward military force."[16]

For NATO, many material and capability-related implications are currently derived from the hypothetical risk "of Russia being tempted to coerce or undertake limited aggression against an Ally in the expectation that it might not elicit a NATO response."[17] It is not necessary to believe that this *is* actually a likely course of action for Russia: even the perception, certainly shared by some of the allies, that it *could* be a viable strategy for Russia is hugely destabilizing. NATO will therefore have to go much farther on its path to military adaption and reassurance. If in 2015 it was noted that Trident Juncture was NATO's biggest exercise in a decade, the following years might bring a requirement to exercise at a much higher level as far as the number of contributing troops is concerned. NATO headquarters used to be full of officers capable of planning and implementing multinational troop movements at the corps level and above. Today, those skills and experience are partly lost and will need to be rebuilt, just as decision-making structures and bureaucratic procedures need to be streamlined and adjusted to the fact that significant international movements of personnel and materiel might have to occur in crisis situations that do not correspond to a legal state of war.

There is also a need for action in the area of conventional military deterrence. This includes the permanent stationing of significant NATO forces in the territory of at-risk member states, ideally in the form of multinational units. The deterrence strategy should not be based exclusively on the assumption that in the event of a crisis, NATO will immediately be able to quickly and easily strengthen its forces. NATO member states have also begun to build specialized military formations to support defense against hybrid attack and deal with hybrid conflict elsewhere. A prominent example is the British 77th Brigade, a combined Regular Army and Army Reserve unit. Recently formed, the 77th Brigade focuses on intelligence, surveillance, and reconnaissance. It is designed to conduct modern information operations, particularly to counter hybrid warfare.

It should be a priority to systematically identify vulnerabilities to hybrid threats so that the currently much-vaunted resilience can be strengthened.

[16] Christian Mölling, "From Hybrid Threats to Hybrid Security Policy," *Ethics and Armed Forces* 2 (2015): 2.

[17] Ruiz Palmer, "Back to the Future," 10.

This may include marginalized groups in society, who may be targets for radicalization efforts or ideological mobilization. It may be a case of energy dependencies that can be turned into means of exerting political pressure. Serious investment is needed in the area of intelligence analysis, security foresight, and weak signals. Another important area of action for defense against hybrid threats is early warning, and to produce a situation assessment that is appropriate for the character of this form of conflict. Here it will be necessary to share and evaluate findings and results of national intelligence service work more rapidly in the international framework within the EU and NATO than is currently the case. Even weak signals pointing to a hybrid attack may consolidate into a pattern if coordination of this kind takes place.

Building up capability in this area will enable NATO to better understand the hybrid threat phenomenon, develop metrics to get a grip on events, systematically address vulnerabilities, and contemplate how hybrid threats might develop in the future. NATO currently lacks the funding mechanisms to take advantage of open-source information that could be provided by think tanks and expert analysts. NATO's public diplomacy budget is spent on events that may or may not have analytical value. NATO ACT has an academic outreach program, but its activities seem better at forming and maintaining networks than using agile partnerships to insert external analysis in NATO processes as and when needed.

Information operations are an integral part of hybrid warfare used to form narratives and, generally, to influence political opinion-making among the target population. Strategic communication offers an opportunity to counteract this, but only if it is coherent, consistent, fast, and precise. While this is certainly not a simple feat, it is surprising to see how difficult NATO and EU seem to find even basic coordination. For example, on 22 June 2015 the EU adopted the Action Plan on Strategic Communication. Back in July 2014, NATO set up the Strategic Communications Centre of Excellence in Latvia for the same purpose. The EU action plan makes no reference to this, while the work plan for 2015 on the NATO center's website does not indicate any prioritization of cooperation with the EU.[18] Meanwhile, however, both organizations have stated that close coordination is needed in precisely this area. With a challenge that confounds traditional categories of analysis, decision-makers and experts alike will need to be creative. The point is not that an event like the invasion of Crimea necessarily forms a template for future conflict, but that the principles on which they were based will inform the next challenger and hybridity as an underlying factor in conflict is here to stay.

[18] European Union, "Action Plan on Strategic Communication," Ref. Ares(2015)2608242, 22 June 2015, http://eap-csf.eu/assets/files/Action%20PLan.pdf (accessed 31 October 2015); NATO Strategic Communications Centre of Excellence, http://www.stratcomcoe.org/about-us (accessed 31 October 2015).

## About the author

Dr. Bastian Giegerich is Director of Defence and Military Analysis at The International Institute for Strategic Studies (IISS) in London. He is a contributor to the IISS's *Military Balance and Strategic Survey*. From 2010 until 2015, Bastian worked for the German Ministry of Defense, both in research and policy roles, while also serving as the IISS Consulting Senior Fellow for European Security. He holds a MA in Political Science from the University of Potsdam and a PhD in International Relations from the London School of Economics. Bastian is the author and editor of several books on European security and defense matters. His articles have appeared in journals such as *Survival*, *Security Studies and International Politics*, among others, as well as in various print media outlets. Bastian has taught International Relations, Military Studies, and Public Administration courses at the London School of Economics, the University of Potsdam, and the University of Kassel. *E-mail*: Giegerich@iiss.org.

*Connections: The Quarterly Journal*
ISSN 1812-1098, e-ISSN 1812-2973

James K. Wither, *Connections QJ* 15, no. 2 (2016): 73-87
http://dx.doi.org/10.11610/Connections.15.2.06

Research Article

# Making Sense of Hybrid Warfare

*James K. Wither*

*George C. Marshall European Center for Security Studies, http://www.marshallcenter.org*

**Abstract**: The term hybrid warfare has been widely analyzed by scholars, policymakers and commentators since Russia occupied Crimea in March 2014. The topic has ceased to be a subject only studied by military strategists, but has entered the wider policy domain as a significant security challenge for the West. This article seeks to place the debate about hybrid warfare in a broader analytical and historical context and summarizes discussion to date on this and related strategic concepts. The Russian approach to hybrid warfare as demonstrated by operations in Ukraine is a particular focus for discussion.

**Keywords**: Warfare, Strategy, Russian Federation, NATO, European Security.

## Introduction

Since the Russian Federation invaded Crimea in March 2014, analysis and commentary on the concept of hybrid warfare have increased exponentially.[1] An Internet search will identify hundreds of entries covering the phenomenon.

[1] Recent analyses include: Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks* (blog), 28 July 2014, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats (accessed 8 December 2015); Max Boot, "Countering Hybrid Warfare," in *Armed Conflict Survey 2015*, ed. Nigel Inkster (London: IISS, 2015); Ralph D. Thiele, "Crisis in Ukraine – The Emergence of Hybrid Warfare," *ISPSW Strategy Series*, May 2015; Rod Thornton, "The Changing Nature of Modern Warfare," *RUSI Journal* 160:4 (2015): 40–48; Lawrence Freedman, "Ukraine and the Art of Limited War," *Survival* 56:6 (2014): 7–38; Michael Kofman and Matthew Rojansky, "Kennan Cable No. 7: A Closer Look at Russia's Hybrid War," *Wilson Center*, 14 April 2015, https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war (accessed 8 December 2015).

Hybrid warfare has become the most common term used to try and capture the complexity of twenty-first-century warfare, which involves a multiplicity of actors and blurs the traditional distinctions between different types of armed conflict and even between war and peace. Hybrid warfare has ceased to be a topic only for military strategists, as it has now entered the broader public domain and become a major security concern for Western governments. Both NATO and the European Union (EU) are working on strategies to strengthen defensive capabilities and prevent hybrid attacks.

This article seeks to clarify the different ways in which the term hybrid warfare and related terms have been used by scholars and policy analysts and summarize discussion on the topic to date. The paper will examine, in particular, the Russian approach to hybrid warfare as demonstrated by operations in Ukraine and will briefly assess the significance of these developments for Western security policy.

## Defining Hybrid Warfare

Not surprisingly, there are many definitions of hybrid warfare. The concept has been delineated in different, if related, ways and these definitions have evolved in a relatively short period of time. Defining hybrid warfare is not just an academic exercise. The way the term is defined may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them.

One approach to hybrid warfare takes an historical perspective. This defines the term simply as the concurrent use of both conventional and irregular forces in the same military campaign. Military historian Peter R. Mansoor, for example, defines hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose."[2] Viewed from this perspective, hybrid warfare is clearly nothing new. There are numerous examples of hybrid techniques and approaches at the tactical, operational and strategic levels stretching back at least as far as the Peloponnesian War and the writings of the Chinese philosopher, Sun Tzu, in the fifth century BC. Irregular fighters have proved to be the bane of numerous conventional militaries. Formidable armies such as Napoleon's Grand Armée and Hitler's Wehrmacht struggled to combat irregular fighters who understood and exploited the local human and geographical terrain and targeted vulnerable logistic bases and lines of communication. Over time, guerrilla operations had a significant and lasting impact on the broader conventional military campaigns of which they were part. Recent counter insurgency (COIN) campaigns in Iraq and Afghanistan have once again highlighted the difficulty of defeating de-

[2] Peter R. Mansoor, "Hybrid War in History," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present,* ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), 2.

termined irregular fighters without committing human rights abuses against the local population and consequently undermining domestic and international public support for the campaign.

During the 2000s, the use of the term "hybrid" became a common way to describe contemporary warfare, particularly because of the increasing sophistication and lethality of violent non-state actors and the growing potential of cyber warfare. Although there was no agreement that this necessarily constituted a new form of warfare,[3] definitions of hybrid warfare emphasized the blending of conventional and irregular approaches across the full spectrum of conflict. For example, in 2007 Frank G. Hoffman, a leading analyst of the concept, defined hybrid warfare as "Threats that incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of non-state actors."[4] During its war with Georgia in 2008, Russia, for example, made use of a combination of regular armed forces, South Ossetian and Abkhazian militias and Russian special operations forces (SOF) operating covertly as "local defense" troops. The mixing of conventional and irregular methods of warfare arguably distinguished such hybrid wars from their historical forms. In the past, conventional and irregular operations tended to take place concurrently but separately, rather than being integrated. In addition, operations by irregular fighters were normally secondary to campaigns by conventional military forces.

Prior to 2014, the conflict between Israel and Hezbollah in 2006 was the most frequently used example of a war that fitted contemporary definitions of hybrid warfare. Hezbollah, which had been trained and equipped by Iran, surprised Israel with its sophisticated combination of guerrilla and conventional military tactics and employed weaponry and communication systems normally associated with the armed forces of developed states. At the strategic level, Hezbollah made effective use of the Internet and other media for information and propaganda. Its information management proved much more successful than Israel's in influencing global opinion from the start of the conflict. As the discussion above illustrates, a hybrid combination of conventional and irregular methods of warfare has been used throughout history. Yet what is apparent from Hezbollah's example and others, including the guerrilla fighters in Chechnya and more recently Islamic State (IS), is that modern weapon systems have greatly increased the lethality of non-state actors. Developments in information technology have also provided these groups with an unprecedented ability to engage in information warfare and compete effectively with states to shape public opinion. The US Quadrennial Defense Review Report in 2010

[3] U.S. Government Accountability Office (GAO), *Hybrid Warfare*, GAO-10-136R (Washington, DC: GAO, 2010), available at http://www.gao.gov/products/GAO-10-1036R (accessed 4 December 2015).

[4] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 8.

acknowledged these changes when it defined hybrid warfare in the following manner: "today's hybrid approaches may involve state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce or intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states."[5]

## Hybrid Warfare Post 2014

As noted above, Russia's actions in Ukraine in 2014 intensified interest in the concept of hybrid warfare. For many Western commentators, "hybrid" appeared to be the best way to describe the variety and blending of tools and methods employed by the Russian Federation during its annexation of Crimea and support to separatist groups in eastern Ukraine. Russian techniques included the traditional combination of conventional and irregular combat operations, but also the support and sponsorship of political protests, economic coercion, cyber operations and, in particular, an intense disinformation campaign. In an interview in July 2014, former NATO Secretary General Anders Fogh Rasmussen described Russian tactics as "hybrid warfare," which he defined as "a combination of military action, covert operations and an aggressive program of disinformation."[6] The 2015 edition of *Military Balance* provides a very comprehensive definition of the latest manifestation of hybrid warfare, highlighting the methods employed, namely "the use of military and non-military tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure."[7]

What distinguishes this definition of hybrid warfare from those discussed earlier is the emphasis on non-military methods of conflict and, in particular, information warfare. The employment of coercive information operations is the most distinguishing feature of the recent descriptions of hybrid warfare and allows some comparisons to be drawn between IS's campaigns in the Middle East and the very different war and theater of operations in Ukraine. IS has effectively blended conventional and guerrilla tactics and gross acts of terrorism, but it has also exploited propaganda and information warfare to an unprecedented extent for a non-state actor. Sophisticated social media campaigns have glorified its cause and high-quality visual propaganda has contributed to the

[5] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 2010), 8, http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (accessed 4 December 2015).

[6] Mark Landler and Michael R. Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine," *The New York Times*, 8 July 2014, www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html (accessed 7 December 2015).

[7] "Complex Crises Call for Adaptable and Durable Capabilities," *The Military Balance* 115:1 (2015): 5.

group's ability to recruit thousands of foreign fighters to its ranks. Information warfare was also central to Russia's successful campaign in Crimea in 2014. At the tactical level, electronic warfare (EW) and cyber attacks neutralized the ability of the Ukrainian authorities to respond, while broader media exploitation techniques blurred the lines between truth and falsehood, creating an alternative reality for those observers who accepted the Russian media's view of events. Russia's strategic information campaign in Ukraine sought to exploit existing societal vulnerabilities, weaken government and state institutions and undermine the perceived legitimacy of the Ukrainian state. Like IS, Russia used information operations to influence and shape public perception, a recognition that the latter has become the strategic center of gravity in contemporary armed conflicts.

It is hardly surprising that Russian analysts have argued that information and psychological warfare are the foundations for victory in what they refer to as "new-generation war."[8] A recent NATO Strategic Communications (STRATCOM) Center of Excellence (COE) report on Russian information warfare in Ukraine drew similar conclusions regarding the significance of "information superiority" to Russia's success,[9] while NATO's Supreme Allied Commander Europe (SACEUR), General Philip Breedlove, reflected the consternation felt by many Western officials when he described the Russian campaign as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[10] According to former Russian TV producer Peter Pomerantsev, this "Blitzkrieg" goes much further than historical information warfare operations. He argues that "The new Russia doesn't just deal with the petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with information warfare. It reinvents reality."[11]

## Related Theories of Contemporary Warfare

Arguably, the concept of hybrid warfare adds little to the notion of asymmetrical warfare. This term, popularized after the Cold War, sought to characterize

[8] For example, see Sergei G. Chekinov and Sergei A. Bogdanov, "The Nature and Content of New Generation War," *Voyenna Mysl (Military Thought)* 4 (2013): 12-23, http://www.eastviewpress.com/Files/MT_from%20the%20current%20issue_No.4_2013.pdf (accessed 9 December 2015).

[9] NATO Strategic Communications Center of Excellence (StratCom COE), *Analysis of Russia's Information Campaign Against Ukraine* (Riga: NATO StratCom COE, 2014), 4, http://issuu.com/natostratcomcoe/docs/ukraine_research_natostratcomcoe_02 (accessed 15 December 2015).

[10] John Vandiver, "SACEUR: Allies Must Prepare for 'Hybrid Warfare,'" *Stars and Stripes*, 4 September 2015, www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464 (accessed 7 December 2015).

[11] Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," *Defense One*, 9 September 2014, http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635 (accessed 10 December 2015).

the kinds of strategies and tactics employed by state and non-state opponents of the US and its allies to counter the West's overwhelming technological advantages and firepower. These asymmetrical methods could naturally shift into non-military fields expanding the grey area between war and peace that Russia has exploited in Ukraine. However, so-called asymmetrical methods of warfare, essentially pitting one's strengths against another's weaknesses, have always been a feature of successful military strategies. Many of the elements identified as hybrid warfare also appear in discussion of "fourth-generation warfare," a contested theory originating in 1990s.[12] A key concept in fourth-generation warfare is the exploitation of emerging information technology, which allows non-state military actors to erode the will of states to fight by targeting decision-makers and the public through the globalized, networked media and the Internet. Thus, widening a "war" to include cultural, social, legal, psychological and moral dimensions where military power is less relevant.

Recent definitions of hybrid warfare are also similar to the Chinese theory of unrestricted warfare. This concept is discussed at length in the book, *Unrestricted Warfare*, which was published in 1999 by two colonels from the People's Liberation Army (PLA).[13] It proposes methods of warfare to enable countries like China to confront an opponent with superior military technology such as the US. Similar to the concept of hybrid warfare, unrestricted warfare involves the use of a multitude of means, both military and non-military, to strike back at an enemy during a conflict. One of the authors stated in an interview that "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[14] Consequently, unrestricted warfare methods include: computer hacking, subversion of the banking system, markets and currency manipulation (financial war), terrorism, media disinformation and urban warfare. The authors, Qiao Liang and Wang Xiangsui, argue that developments in information technology and globalization have conclusively changed the conduct of war, which has consequently moved beyond the military realm to a "new concept of weapons," such as the use of computer viruses during combat operations.[15] These "new" techniques of warfare are curiously referred to as "kinder weapons," but the aim of their use remains Clausewitzian, that is to compel an opponent to bend to China's will. As a quotation from "Unrestricted Warfare" explains: "a kinder war in which bloodshed may be avoided is still

[12] Tim Benbow, "Talking 'Bout Our Generation? Assessing the Concept of Fourth-Generation Warfare," *Comparative Strategy* 27:2 (2008): 148–163. Even more contested is the notion of "Fifth Generation Warfare," on which readers can see for example Donald J. Reed, "Beyond the War on Terror: Into the Fifth Generation of War and Conflict," *Studies in Conflict and Terrorism* 31:8 (2008): 684–722.

[13] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 2, https://www.oodaloop.com/documents/unrestricted.pdf (accessed 15 December 2015).

[14] Ibid., 2.

[15] Ibid., 25.

war. It may alter the cruel process of war, but there is no way to change the essence of war, which is one of compulsion, and therefore it cannot alter its cruel outcome, either."[16] The extent to which unrestricted warfare has become official Chinese doctrine is not clear. However, recent reports suggest that these techniques may be evident in China's "three warfares" approach to its territorial claims in the East and South China seas.[17]

## Are Non-Military Hybrid Methods Really Warfare?

Hybrid warfare tends to be used to describe all wars that are not strictly conventional, namely waged between the legally constituted armed forces of nation-states. Arguably, therefore, the term hybrid warfare is too vague to be of practical use to analysts and policymakers. As Latvian analyst, Jānis Bērziņš, notes "The word hybrid is catchy, since it may represent a mix of anything."[18]

The inclusion of a range of non-military means in a definition of hybrid warfare runs the risk of describing normal inter-state competition and conflict as war even in the absence of the threat or use of violence. A realist concept of international politics already posits inter-state relations as naturally competitive and conflictual. An environment in which sovereign states, primarily concerned with their security, act in pursuit of their national interests and struggle for power, cooperating and competing with other states as necessary to best achieve their objectives. The usual economic, diplomatic and informational measures used in inter-state competition are not normally classified as warfare in the absence of the threat or actual use of force. However, many of the statements emanating from Russia's government and media suggest that Russia perceives itself as at "war" with Western democracy, culture and values.[19] This development suggests that, at least for the foreseeable future, Russia has returned to a Soviet-era style battle of ideas with the West where, to reverse Clausewitz, peace is essentially a continuation of war by other means. Rod Thornton has suggested that the West must adjust to a situation where it is in a "permanent" state of hybrid war with Russia.[20] However, war in this context is

[16] Ibid., 30.

[17] See for example: John Garnaut, "US Unsettled by China's Three Warfares Strategy: Pentagon Report," *The Sydney Morning Herald*, 11 April 2014, www.smh.com.au/federal-politics/political-news/us-unsettled-by-chinas-three-warfares-strategy-pentagon-report-20140410-36g45.html (accessed 16 December 2015); and James R. Holmes, "Exposing China's Provocations," *The Diplomat*, 28 August 2014, http://thediplomat.com/2014/08/exposing-chinas-provocations (accessed 16 December 2015).

[18] Jānis Bērziņš, "A New Generation of Warfare," *Per Concordiam* 6:3 (2015): 24, http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V6N3_en.pdf (accessed 9 December 2015).

[19] "Russia's War on the West," *The Economist*, 14 February 2015, www.economist.com/news/leaders/21643189-ukraine-suffers-it-time-recognise-gravity-russian-threatand-counter (accessed 17 December 2015).

[20] Thornton, "The Changing Nature of Modern Warfare," 45.

arguably the status quo of international politics and it is misleading and potentially dangerous to describe Russia's broader aims and methods simply as a form of warfare. Analyst Ralph Thiele, for example, includes Russian investments in key sectors of European economies and Russian organized crime links with local criminal elements in the Russian model of hybrid war.[21] In this author's opinion, only when non-military methods are coordinated or integrated with the actual threat or use of armed force should policymakers describe international political rivalry as a form of hybrid warfare. Naturally, a response to a real threat of hybrid warfare would require a comprehensive or "whole of government" effort, as non-conventional methods of warfare cannot be addressed by military means alone. It is probably a stretch to classify efforts to target corrupt Russian officials as a form of "warfare," although it might certainly be an element of soft power employed by Western states in their competition with Vladimir Putin's Russia. Overall, it is worth remembering that even at the height of the Cold War, the Soviet Union and the US were able to temper their rivalry to pursue mutually beneficial nuclear arms control agreements and limit proxy wars.

## New Generation Warfare: Russia's Hybrid Warfare

Like the authors of *Unrestricted Warfare*, Russian analysts make no secret that their objective is to advocate approaches to warfare that will counter perceived overweening and threatening US power. Many Russian commentators and analysts claim that Russia has been under sustained and effective information attack by the US since the 1980s. Events such as perestroika and the "color revolutions" and multilateral organizations such as the IMF and World Bank are all considered instruments of irregular warfare intended to destabilize Russia.[22] From a Russian perspective, the seizure of Crimea and operations in eastern Ukraine are strategic defensive campaigns to counter US hybrid warfare against its national interests and values.

Hybrid warfare is a Western term, not a Russian one. When Russian analysts write on the subject, they use the terms "new generation warfare" or "non-linear war." The former was introduced to Western audiences through a paper published by General Valery Gerasimov, the Chief of the Russian General Staff, in February 2013. Consequently, the Russian approach to hybrid war is sometimes referred to inaccurately as the "Gerasimov Doctrine." Gerasimov describes new generation warfare as: "the broad use of political, economic, informational, humanitarian and other non-military means … supplemented by

[21] Thiele, "The Crisis in Ukraine," 6.

[22] Bērziņš, "A New Generation of Warfare," 23; and Bret Perry, "Non-Linear Warfare in the Ukraine: The Critical Role of Information Operations and Special Operations," *Small Wars Journal*, 14 August 2015, http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera (accessed 9 December 2015).

civil disorder among the local population and concealed armed forces."[23] Gerasimov recognizes that many of the methods he identifies were not traditionally part of what would be considered wartime activities. However, he believes that they are typical of twenty-first-century warfare and actually more significant for the achievement of strategic goals than military means because they can reduce the fighting potential of an enemy by creating social upheaval and promoting a climate of collapse without the overt use of violence.[24] Nevertheless, it is evident from Gerasimov's paper that the armed forces have an essential supplementary role in new generation warfare. This is particularly the case with special operations forces (SOF) that can be used under the guise of "peacekeeping and crisis regulation" to link up with opposition groups inside a targeted state.[25] In their discussion of new generation warfare, analysts Sergei G. Checkinov and Sergei A. Bogdanov also envisage the employment of SOF in "large-scale reconnaissance and subversive missions under the cover of the information operation."[26]

The use of SOF under cover of information operations was clearly evident in Ukraine in 2014. Covert *spetsnaz* units (the "little green men") were employed to seize government buildings and key infrastructure targets and arm separatist militia, while the Russian government spread doubt and confusion through repeated denials of Russian involvement. Other techniques of hybrid or new generation warfare were used to demoralize and intimidate opponents. These included exercises by Russian conventional forces close to the Ukrainian border, cyber attacks on Ukrainian government systems and a wider diplomatic and media offensive to undermine the legitimacy of the new government of Ukraine. The ultimate aim of this sort of "warfare" is to apply psychological pressure to cause the collapse of the target state from within so that the political objectives of the conflict can be achieved without fighting – the acme of strategic skill according to Sun Tzu. Bērziņš accurately sums up the Russian approach to modern warfare as follows:

> … the main battlespace is in the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare … The main objective is to reduce the necessity for deploying hard military power to the minimum necessary, making the opponent's military and civil population support the attacker to the detriment of their government and country.[27]

[23] General Gerasimov's article is available in English from Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (accessed 11 December 2015).

[24] Ibid., 2–3.

[25] Ibid., 3–4.

[26] Chekinov and Bogdanov, "The Nature and Content of New Generation War," 20.

[27] Jānis Bērziņš, *Russian New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga: National Defence Academy of Latvia, 2014), www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx (accessed 14 December 2015).

Many of the methods Russia has used in Ukraine date back to the Soviet era and the application of *maskirovka*, or military deception. This was effectively applied by Soviet forces during World War II and in Cold War proxy conflicts. For example, *maskirovka* was used on a grand scale in Operation Bagration in 1944 when an entire German Army Group was destroyed. At the other end of the conflict spectrum, *maskirovka* techniques were employed in Eastern Europe after 1945 when Soviet interior ministry troops (NKVD) used covert means to take over state institutions, undermine civil society and crush all opposition to the imposition of Communist rule.[28] In the twenty-first century, advances in information technology and processing have greatly increased the scope of *maskirovka,* allowing the Russian government to employ multimedia propaganda and misinformation on a massive scale. These have been used to build support for the government's foreign policy within Russia and to wage a wider "information war" against Ukraine and the West. In the current NATO context, Julian Lindley-French defines *maskirovka* as "war that is short of war, a purposeful strategy of deception that combines use of force with disinformation and destabilisation to create ambiguity in the minds of Alliance leaders about how best to respond."[29]

The concept of "reflexive control" (perception management) is a key element of *maskirovka.*[30] This originated with the work of former Soviet psychologist Vladimir Lefebvre who developed the theory while researching ways to influence and control an enemy's decision-making processes. The theory can be described as the use of specially-prepared information that inclines an opponent to voluntarily make a decision that has been predetermined as desirable by the initiator of the information. Methods include blackmail, camouflage, deception and disinformation, all intended to interfere with an opponent's decision-making cycle in a way favorable to Russian policy. The continued post-Soviet interest in reflexive control techniques was demonstrated by the launch of a new security studies journal entitled *Reflexive Processes and Control* as recently as 2001.[31]

In practice, the execution of new generation warfare poses significant challenges. A wide range of parties—civil and military, regular and irregular, as well

[28] For a detailed account of this process see: Anne Applebaum, *Iron Curtain: The Crushing of Eastern Europe 1944–1956* (London: Allen Lane, 2012).

[29] Julian Lindley-French, *NATO: Countering Strategic Maskirovka* (Calgary: Canadian Defence and Foreign Affairs Institute, 2015), 4, http://www.cgai.ca/nato_countering_strategic_maskirovka (accessed 8 December 2015).

[30] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17 (2004): 237–256; and Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, 2015), http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (accessed 11 December 2015).

[31] Thomas, "Russia's Reflexive Control Theory and the Military," 237.

as their activities—must be coordinated, integrated and controlled to achieve the overall military and political objectives. Unified political control is especially difficult, as irregular and state actors often have differing political interests. Even for an authoritarian state such as Russia, control and coordination proved difficult during operations in Ukraine, which appear to have been less well-orchestrated than many Western commentators believed at the time.[32] For example, analysis by the Wilson Center concludes that Russian actions in Ukraine were not part of a well-coordinated master strategy, but rather reflected "the unplanned succession of different tools to fit different—often unexpected—operational realities."[33]

## Russian Hybrid Warfare as a Threat to NATO

Much concern has been expressed about NATO's vulnerability to Russian hybrid warfare techniques. Naturally, the security of the Baltic States, with their significant Russian-speaking minorities, is of particular concern. It has been longstanding Russian policy to weaken, divide and ultimately neutralize NATO. The Baltic States provide Putin with the potential leverage to achieve this aim. Just as Russian meddling in Ukraine started long before the annexation of Crimea, political and social pressure has been ratcheted up in the Baltic States.[34] Some European intelligence agencies have also expressed fears about Bulgaria, where the entire political system is believed to be compromised by criminal organizations linked to the Russian state by Russian intelligence agencies.[35] NATO strategy to combat Russian hybrid warfare needs to combine diplomatic, military, informational, economic and law enforcement efforts. Yet such a comprehensive approach must be properly integrated, rather than simply involving civilian agencies in support of military forces or replacing armed forces with civilian measures due to a reluctance to deploy the former.

In a crisis involving the Baltic States, Russia would likely seek to divide NATO members by staying below an obvious Article 5 threshold, at least initially. As during the Ukraine crisis in 2014, disinformation, intimidation and propaganda would be used to try to encourage the less robust members of NATO to accept the Russian version of events, which would, of course, conveniently reinforce their existing inclination to avoid a military response. Disinformation would be used against NATO governments and wider public opinion to keep the Alliance politically and militarily off-balance. Intimidation would likely highlight Russia's

[32] Freedman, "Ukraine and the Art of Limited War," 11; Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[33] Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[34] See for example Andrew Osborn, "Putin a Threat to Baltic States, Western Officials Say," *Reuters*, 19 February 2015, http://uk.reuters.com/article/uk-britain-russia-baltics-idUKKBN0LN0FT20150219 (accessed 18 December 2015).

[35] Sam Jones, "Ukraine: Russia's New Art of War," *Financial Times*, 28 August 2014, http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html (accessed 10 December 2015).

apparent willingness to employ nuclear weapons to de-escalate NATO "aggression." Effective strategic communication could counter Russian narratives, but it would need to be responsive, coherent and consistent. Although the EU adopted a strategic communication action plan in 2015, there is no evidence that EU planning includes coordination with the NATO'S STRATCOM COE, which was founded in 2014.[36] Such coordination would be vital to respond effectively to a Russian disinformation and propaganda campaign. Unfortunately, authoritarian societies have an advantage, as they can more easily mobilize all of the resources of the state for political purposes without the restrictions imposed by a decentralized distribution of power and a democratic consensus-building process. In contrast, liberal democracies have a distaste for propaganda and psychological warfare and the NATO alliance would find it difficult to agree on the content and presentation of a strategic communication campaign. As the STRATCOM COE acknowledges, Russia has a potential asymmetrical advantage over the West, as the latter's free media cannot compete with centrally-controlled and synchronized Russian information warfare operations.[37]

However, NATO may not be as vulnerable to information warfare as many believe. Propaganda can have a particularly strong effect when a population, as in Russia, is denied alternative sources of information, but elsewhere propaganda must be plausible enough to shape beliefs and emotions and exploit general uncertainty, mistrust and paranoia. Russian government pronouncements and media sources have become increasingly discredited in the West, especially since their responses to the shooting down of flight MH 17 over Ukraine in July 2014. Increased control of the national media and the Internet as well as harassment of dissenters made it possible to shape Russian public opinion. However, despite the efforts of Russia Today (RT) and a veritable army of Internet trolls to contradict and abuse news outlets and social media that take anti-Russian positions, Russian information operations have largely failed to influence non-Russian-speaking audiences.[38] Ukrainian government sources claim that there is now a very low level of public confidence in any official Russian media,[39] and despite Russia's intense information campaign, support for pro-Russian separatists even amongst Russian-speaking Ukrainians was lower

[36] Bastian Giegerich, "Hybrid Attacks Demand Comprehensive Defence," *Ethics and Armed Forces* 2 (2015): 15, http://www.ethikundmilitaer.de/fileadmin/Journale/2015-12_English/Hybrid_Warfare-Enemies_at_a_Loss_2015-2.pdf (accessed 9 December 2015).

[37] StratCom COE, *Analysis of Russia's Information Campaign Against Ukraine*, 3.

[38] Freedman, "Ukraine and the Art of Limited War," 23; and Snegovaya, "Putin's Information Warfare in Ukraine," 18–20.

[39] "Sociology of Information Warfare in Ukraine," *Europe Insight*, 11 October 2015, http://en.europeinsight.net/sociology-of-information-warfare-in-ukraine (accessed 10 December 2015).

than anticipated. This partly explains Russia's need for more overt military involvement in the conflict in the summer of 2014.[40]

During crisis, Russian tactics will likely involve covert support to local pro-Russian activists. As in Ukraine, ambiguity and deniability will make it difficult to confirm that an attack is under way. The following quotation from Mark Galeotti starkly illustrates the potential difficulties of responding to these methods, especially forcefully:

> The first little green man, after all, might instead be a 15-year-old Russian-Estonian girl waving a "Russian-speakers have rights, too" placard in the border city of Narva. Shoot her? Of course not. The second might be her older brother, throwing rocks at the police coming to arrest her. Shoot him? Hopefully not, especially as you can guarantee that footage of the incident would promptly be blasted across Russian TV channels.[41]

Paramilitary police would probably be better equipped and trained than soldiers to handle such situations, which is another example of where closer cooperation between the EU and NATO would undoubtedly be beneficial.

If a crisis were to escalate, Russia might be tempted to seize territory in vulnerable frontline states by overt military means before the Alliance could mount an effective collective response.[42] The nightmare scenario for NATO would be the occupation of part of a member state, even if temporarily. Such action would force the Alliance to invoke Article 5 of the Washington Treaty and risk a direct armed confrontation with a nuclear-armed Russia or fail to respond to the aggression and risk the collapse of NATO as a viable military alliance. Despite the misgivings of states such as Germany, effective deterrence will require the permanent stationing of significant multinational forces on the territory of states that might be at risk in order to deny Russia the option of a military fait accompli. Although NATO's new 5,000-strong Very High Readiness Joint Task Force (VJTF) should be able to deploy rapidly, it may still arrive too late to deter Russian adventurism. The Russian approach to hybrid warfare does not exclude the direct use of military force when necessary. In summer 2014, when Russia had exhausted its use of non-military hybrid methods, military operations in Ukraine took on the character of limited conventional war. Russian battalion tactical groups (BTG) intervened directly in combat against the Ukrainian army. Fighting involved clashes between armored forces, intense urban infantry battles, heavy artillery barrages and, at least on the Russian side, the employment of "drones" for surveillance and target acquisition, electronic

[40] Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[41] Mark Galeotti, "Time to Think About Hybrid Defense," *War on the Rocks*, 30 July 2015, http://warontherocks.com/2015/07/time-to-think-about-hybrid-defense (accessed 8 December 2015).

[42] See Elbridge Colby and Jonathan Solomon, "Facing Russia: Conventional Defence and Deterrence in Europe," *Survival* 57:6 (2015): 23–24.

warfare and air defense assets.[43] NATO troops have already started to learn from the experiences of Ukrainian soldiers about Russian tactics and technologies, in particular the use of drones to direct artillery fire and Russian electronic jamming capabilities.[44] However, such tactical improvements alone are unlikely to be enough to provide credible conventional deterrence against armed attack.

## Conclusion

Hybrid warfare does not change the nature of war. Violence remains at the core of hybrid warfare as it does any other form of war, and its aim is the same as any other act of war, namely, to exploit the threat or use of organized violence to gain physical or psychological advantages over an opponent. However, the plethora of terminology—hybrid, asymmetrical, unconventional, non-linear, new generation, fourth and fifth generation, grey wars etc.—reflects the difficulties that strategists and scholars continue to have in categorizing the complex armed conflicts of the twenty-first century. Although the term "hybrid" is currently the most popular, it is by no means the only one to describe these wars. The fact that many armed conflicts blur the lines between war and peace and involve the use of instruments that were not traditionally part of warfighting further complicates the problem. It is undoubtedly a challenge for traditional security establishments to address the wide range of threats identified by the analysts and scholars of hybrid warfare. Cast the definitional net too wide, and a term like hybrid warfare becomes too all-encompassing to be of any practical use to policymakers. Define warfare too narrowly, and policymakers may fail to appreciate the significance of many non-traditional techniques of warfare that are being employed by an adversary as a prelude or adjunct to the use of military force.

Regardless of how the threat is labelled, strategists must decide how best to address the methods employed by their adversaries, whether state or non-state actors. Sometimes the most appropriate responses may involve the application of specific political, informational, economic, diplomatic or, in the case of a physical threat, military tools of statecraft. More complex threats require a whole of government or comprehensive approach. Usually, the best strategies involve the coordination and direction of all of the effective instruments of state power, no matter how the threat is defined. Undoubtedly, NATO needs to enhance its military deterrence capability, but in the case of the West's adversarial relationship with Putin's Russia, the temptation to describe this rivalry as

[43] Philip A. Karber, *Lessons Learned from the Russo-Ukrainian War* (Vienna, VA: The Potomac Foundation, 2015).

[44] "Situation Report," *Foreign Policy*, 10 December 2015, http://foreignpolicy.com/2015/12/10/situation-report-carter-gets-through-another-hill-appearance-new-book-by-former-intel-chief-nato-training-against-russian-tactics-india-comes-to-the-pentagon-house-wants-to-supply-kurds-new-nort (accessed 14 December 2015).

hybrid warfare may inflame an already challenging security situation and blind governments to potentially productive traditional diplomatic policy initiatives.

## About the author

Professor Wither is a retired British Army officer and former researcher in 20th century warfare at the Imperial War Museum in London. He has taught terrorism, warfare and related security studies subjects at a wide variety of institutions, including the FBI Academy, the UK Defence Academy, the NATO School, the NATO Centre of Excellence – Defence Against Terrorism (COE-DAT), the Geneva Centre for Security Policy and various staff colleges and military universities in Europe and Eurasia. *E-mail*: witherj@marshallcenter.org.

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Joshua P. Mulford, *Connections QJ* 15, no. 2 (2016): 89-107
http://dx.doi.org/10.11610/Connections.15.2.07

**Research Article**

# Non-State Actors in the Russo-Ukrainian War

***Joshua P. Mulford***

*US Army, http://www.army.mil/*

**Abstract**: The current war in Ukraine has highlighted the fact that in this new age of warfare non-state actors play a larger role than ever before. The influence of the media, think tanks and academia, religious groups, organized crime, war militias, NGOs and GONGOs, and the Ukrainian diaspora is pervasive. Kremlin-controlled media coverage of the war in Eastern Ukraine, including the downing of the MH-17 jet, is offset by the newer grassroots pro-Ukrainian media outlets such as Ukraine Today. Think tanks and academia focused on Ukraine and Russia are also battling for visibility in the government and among the populous.

The impact of religious groups on the Ukrainian conflict is best featured in the Russian Orthodox Church's rationalizing the invasion of Crimea as Russia's divine right. The Ukrainian church, a subset of the ROC, has broken off and played a proactive role in assisting the war effort by pro-Ukrainian militias. The almost concurrent rise of militias and organized crime in Ukraine pose as a precarious issue for the future of the country. As the government is incapable of regaining sovereignty of its territory, stand-alone militias have risen to fight the Russian invasion in Eastern Ukraine. Organized crime has capitalized on the instability of the region, and with the annexation of Crimea, a new system of black market activities has been opened. The outside world is taking an interest in the Ukrainian plight, as well as in the form of NGO support, and in the case of Russia, GONGOs to promote policies in line with their agendas. The Ukrainian diaspora has also fought to influence policy making towards Ukraine, forming committees and sending supplies to the front line.

It is unclear how much influence these non-state actors will have in the future of Ukraine, but it is quite certain that they each play a significant role in the way the conflict is perceived.

**Keywords**: Non-state actors, Ukraine, Crimea, Russo-Ukrainian war.

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

## Introduction

Non-state actors have played a significant role in creating and influencing the current war in Ukraine. From competing narratives broadcasted by media outlets to misinformation campaigns designed to confuse and cause fear, the media strive to gain the advantage of discourse. Likewise, think tanks and academia influence not only public discourse, but political agendas and, ultimately, policy. Religious groups also take sides either by supporting Ukrainian citizens adversely affected by the conflict or actively participating in promoting a nationalistic narrative with religious and historical themes.[1] The Russo-Ukrainian War and illegal occupation of Crimea have created opportunities for organized crime to flourish in the vacuum left by the Ukrainian government's inability to control its sovereign territory. On both sides of the war militias have quickly organized and are often more effective than government forces. Non-governmental and government organized non-governmental organizations (NGOs and GONGOs) play a variety of roles within Ukraine, while also bearing transnational influence. The Ukrainian diaspora continues to provide varied levels of support for their native country. The extent to which non-state actors will have an impact on the outcome of the conflict is yet to be determined; however, non-state actors have and will continue to play a significant role from the battlefields of eastern Ukraine to the halls of the US Congress.

## Media

Russian mass media is controlled by the Kremlin. This is a characteristic of autocratic states that fear counter-narratives to the government's approved messaging. As President Vladimir Putin observed the waves of social unrest over the last decade, from color revolutions to the Arab Spring, he became aware of the power of social media and messaging in the new domain of war – information space. *Russia Today* (RT) and *Channel One* are two of the largest state-owned television networks that broadcast pro-Russian multilingual programming worldwide. Russia has transformed a traditional non-state actor into an instrument of the state to shape domestic and foreign opinion and silence the opposition.

The use of media to demoralize, confuse and delay opponents was most notably seen after the downing of flight MH17. Western media networks asserted, based on initial evidence, that Russian troops or Russian-backed separatists were responsible. Russian mass media quickly put into question initial claims by accusing Ukrainian troops or NATO forces of the act. This use of disinformation created conspiracy theories that diminished the truth.[2]

[1] Mykhailo Cherenkov, "Orthodox Terrorism," *First Things*, May 2015, available at www.firstthings.com/article/2015/05/orthodox-terrorism (accessed 20 March 2016).

[2] John Lough, *et al.*, *Russian Influence Abroad: Non-state Actors and Propaganda* (London: Chatham House, 2014), 8–9, available at http://www.chathamhouse.org/sites/

RT was established in 2005 to familiarize the world with the Russian viewpoint. In 2015, the network enjoyed a budget of $275 million provided by the Russian government. Notwithstanding its massive budget, RT has not been as effective as Russia had hoped, and is now considered a laughable source of information.[3] In fact, in March 2014 news anchor Liz Whal resigned on air in opposition to the "whitewashing" of events by the Russian government, stating that it was against her morals and ethics as a journalist to continue working at RT.[4] The network continues to provide extensive coverage of the situation in Ukraine and greatly influences opinions of Russians and Ukrainians, especially in Crimea and eastern Ukraine, where Russia censors any pro-Western media.

Ukraine, along with the West, is struggling to find an appropriate response to Russia's advantage in the information space. However, despite spending billions of dollars on propaganda campaigns, Russian media are losing credibility, and the international community has a lower perception of Russia than before Ukraine's Revolution of Dignity. Unified Western action in Ukraine has been slow much to the delight of Russian authorities, but any good will toward Russia that existed prior to 2013 has been lost. A Pew research poll conducted in April and May 2015 found that of the eight NATO counties surveyed, only 26 percent of respondents had a favorable opinion of Russia.[5] The misunderstanding of the information space by the Russian state-sponsored media has shown the importance of free media's role as a non-state actor in building trust and a believable dialogue with the international community.[6]

The late Boris Nemtsov's daughter, Zhanna Nemtsova, has claimed Russian propaganda killed her father, saying, "It kills reason and common sense but it also kills human beings." Nemtsov had been preparing a report that would challenge Putin's claim that there were no Russian troops in Ukraine. However, he was gunned down outside the Kremlin on 27 February 2015, days before he was supposed to lead an anti-war rally against Russia's actions in Ukraine. For years, Russian media demonized opposition figures like Nemtsov as "national traitors," known in Russia as the "fifth column." In some instances, propaganda may be severe enough to incite people to commit unthinkable acts of violence,

files/chathamhouse/field/field_document/20141024RussianInfluenceAbroad.pdf (accessed 18 July 2015).

[3] Ivan Nechepurenko, "Russia Only Has Itself to Blame for Lost Influence in Post-Soviet Sphere," *The Moscow Times*, 30 June 2015, http://www.themoscowtimes.com/news/article/russia-only-has-itself-to-blame-for-lost-influence-in-post-soviet-sphere/524757.html (accessed 1 July 2015).

[4] Liz Whal, "RT Anchor Quits on Air," YouTube video, 5 March 2014, https://www.youtube.com/watch?v=55izx6rbCqg (accessed 3 July 2015).

[5] Nechepurenko, "Russia Only Has Itself to Blame."

[6] Mark Galeotti, "The West Is Too Paranoid about Russia's 'Infowar,'" *The Moscow Times*, op-ed, 30 June 2015, www.themoscowtimes.com/opinion/article/the-west-is-too-paranoid-about-russias-infowar-op-ed/524756.html (accessed 1 July 2015).

as was the case in Nazi Germany, Rwanda and now in Ukraine.[7] Nemtsov's murder was significant as he was a major opposition figure outspoken in his condemnation of the Russian annexation of Crimea and support for separatists in eastern Ukraine.

Meanwhile, the *Ukraine Today* network was founded in August 2014 as a Kyiv-based English news outlet with the goal of strengthening "international communications, understanding, and peace."[8] At the Black Sea Security Conference in Bucharest, Strategic Communications Director Lada Roslycky appealed to the participants to stop calling what is going on in Ukraine as a crisis or conflict and call it what it is – a war.[9] News outlets such as *Ukraine Today* and *Kyiv-Post* provide media coverage to influence international perception of the situation in Ukraine.[10] Both provide a wide range of platforms to present a different perspective to the Russian narrative.

There are grassroots efforts to combat Russian propaganda within Ukrainian civil society. *StopFake.org* is an online community created by alumni and students from the Mohyla School of Journalism in Kyiv. This group of independent journalists is determined to protect the integrity and honesty of information that is found in the media about Ukraine. As of April 2015, journalists at *StopFake.org* had verified over 1,000 pieces of media and identified 400 pieces of false reporting.[11] *StopFake.org*'s work remains incredibly important by keeping Russian media in check and providing readers with an accurate story.

Founded in 1949 as an anti-Communist news network, *Radio Free Europe / Radio Liberty* (RFE/RL) initially received funds from the CIA. Currently, it receives funding from the Board of International Broadcasters (BIB), which is backed by the U.S. Congress. Despite the funding source, the BIB acts as a buffer between government and program content. The goal of the network is to spread information where open media is not allowed – mostly in autocratic, closed societies.[12] RFE/RL has delivered significant reporting on the war, primarily seeking to influence Russian speakers in Ukraine.

The role of media in Ukraine has proven to shape what people know and influence how they act. Evidently, the restriction by Russian and pro-Russian authorities in Crimea and eastern Ukraine of various media outlets also plays into shaping the knowledge of society. Despite all of Russia's best attempts to promote one common pro-Russian story, independent and grassroots efforts are

[7] Zhanna Nemtsova, "My father was killed by Russian propaganda, says Nemtsov's daughter," *The Guardian*, 19 June 2015, http://www.theguardian.com/world/2015/jun/19/russia-boris-nemtsov-zhanna-nemtsova (accessed 30 June 2015).

[8] *Ukraine Today*, http://uatoday.tv/about (accessed 30 June 2015).

[9] In honor of the realities on the ground and in respect for Ms. Roslycky's appeal in the paper the author prefers to label the current conflict in eastern Ukraine, the Russo-Ukrainian War.

[10] Lada Roslycky, "Black Sea Security Program," 26 May 2015, Bucharest, Romania.

[11] http://www.stopfake.org/en/about-us/.

[12] *Radio Free Europe / Radio Liberty*, http://www.rferl.org/info/about/176.html.

gaining momentum and leaving their own impact on the coverage and narrative of the conflict.

## Think Tanks and Academia

Ukrainian and international think tanks are having a profound impact on domestic government reforms and are externally shaping the dialogue on how the international community should support the government in Kyiv and react to Russian aggression. Since the fall of the Soviet Union, think tanks in Ukraine such as the Ukrainian Centre for Economic and Political Studies (The Razumkov Centre), The Atlantic Council of Ukraine and The Europe XXI Foundation have enjoyed considerable political independence. The Institute for Economic Research and Policy Consulting (IER) is particularly well-known independent Ukrainian think tank. Reports developed by the IER include the effects of abolishing visa requirements for travel through the EU for Ukrainians, investment forecasts by region and the impact of the Deep and Comprehensive Free Trade Agreement (DCFTA) on various levels of Ukrainian society.[13] The IER's role of providing in-depth analysis to policymakers and potential investors alike during a time of war should be highlighted. Its reports have a direct impact on the decisions of leaders, which have grave and long-lasting consequences for the viability of Ukraine.

A product of the Revolution of Dignity was the creation of the non-partisan NGO, Maidan of Foreign Affairs (MFA). Diplomats and experts who openly opposed Viktor Yanukovych government created MFA to discuss policy based on democratic ideals. MFA's main objectives are to provide expert opinion on foreign policy and national security, educate the public on key issues and promote greater policy debate. MFA has produced intelligence manuals for the army that are being used on the battlefields in eastern Ukraine as well as for formulating a strategy to regain Crimea.[14]

Russian think tanks and academia have increasingly become less independent as the government seeks to control them. Over time, their conclusions and instructions have become more aligned with the goals and narratives of the Kremlin. Individuals who fail to operate within the approved narrative face intimidation, and often choose to flee Russia. Former Provost of the New Economic School in Moscow, Sergei Guriev, now teaches in Paris after he was notified his lessons were not appreciated by the Kremlin. In 2015, the Russian parliament passed a law on "undesirable" organizations that threatened the security and order of Russia. Organizations that have been investigated as "undesirable" include Amnesty International, the Carnegie Foundation and Human Rights Watch. The new legislation has created a threatening environment for top Russian economists and experts leading to a brain drain, weakening the in-

[13] The Institute for Economic and Policy Consulting, www.ier.com.ua/en/projects/.

[14] *The Maidan of Foreign Affairs*, http://mfaua.org/about/?lang=en (accessed 1 July 2015).

ternal dialogue inside Russia.[15] This lack of domestic debate has led to a self-perpetuating relationship between government, think tanks and academia.

The most influential Russian think tank is the Russian Institute for Strategic Research (RISI) that openly supported the 2014 invasion of Ukraine. RISI has former ties to Russia's Foreign Intelligence Services (SVR) and thus remains a trusted source of expertise to the Kremlin. Additionally, RISI believes that the Russian Federation is the center of gravity in the former Soviet space, a counter-narrative to the international order led by the US, which believes all countries have the right to self-determination and sovereignty regardless of their size.[16] The Russian narrative, called the "Russian World," in which Putin and the Russian Federation act as the sole security guarantor of Russian speakers everywhere, has played out in Ukraine as Putin maneuvers to ensure Ukraine looks east before looking west. As Russian think tanks continue to be investigated and labeled "undesirable," it is important to take heed of the consequential role that groups like RISI play and their effect on influencing policy toward Ukraine.[17]

Think tanks outside Ukraine and Russia, such as the Washington-based Atlantic Council, Brookings Institute and Potomac Foundation strive to keep the attention of lawmakers on the dire situation in Ukraine with comprehensive expert coverage. These practitioners, professors and specialists lead panels at congressional hearings and develop thought-provoking reports that ignite policy discussion in the media and on Capitol Hill. For example, the Atlantic Council, Brookings and The Chicago Council on Global Affairs collaborated to produce a report titled *Preserving Ukraine's Independence, Resisting Russian Aggression: What the United States and NATO Must Do*.[18] The report carried significant weight due to the high level of experience and expertise that was leveraged to produce and support it, and ultimately calls for greater US support for Ukraine in the form of lethal aid.

[15] Andrei Kolesnikov, "Russia's Brain Drain: Why Economists Are Leaving," Carnegie Moscow Center, 26 May 2015, http://carnegie.ru/publications/?fa=60221 (accessed 1 July 2015).

[16] Barack Obama, "Full Transcript: President Obama Gives Speech Addressing Europe, Russia on March 26," *The Washington Post*, 26 March 2014, https://www.washingtonpost.com/world/transcript-president-obama-gives-speech-addressing-europe-russia-on-march-26/2014/03/26/07ae80ae-b503-11e3-b899-20667de76985_story.html (accessed 19 July 2015).

[17] Paul Goble, "Russian Think Tank That Pushed for Invasion of Ukraine Wants Moscow to Overthrow Lukashenka," *Eurasia Daily Monitor*, 27 January 2015, www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=43458 (accessed 1 July 2015).

[18] Ivo Daalder, *et al.*, *Preserving Ukraine's Independence, Resisting Russian Aggression: What the United States and NATO Must Do* (Washington, DC: The Atlantic Council, 2015), http://www.atlanticcouncil.org/images/files/UkraineReport_February2015.pdf (accessed 30 June 2015).

The Atlantic Council's follow-up report, called *Hiding in Plain Sight*, documents evidence of Russian involvement in the ongoing war in Ukraine and was published in May 2015, the same month as the better-known Nemtsov report, appropriately titled *Putin War*.[19] Both provide motives for Russian aggression, how Russia has executed the war and evidence based on photography, tapped phone conversations, interviews and social media. These reports have had minimal impact inside Russia, as Russian citizens care little about Russia's involvement in Ukraine and the government is unlikely to acknowledge military operations in response to the evidence provided by the late Nemtsov.[20] Conversely, the reports have had a significant effect on policymakers on Capitol Hill, routinely referenced as lawmakers continue to put pressure on the Obama administration to provide lethal aid to the Ukrainian armed forces.

The Potomac Foundation provided break-through reporting and analysis on Russia's hybrid war in Ukraine in March 2015. The report was based on President Phillip A. Karber's personal experience on the front lines of the war in the Donbas region. The Ukrainian government requested an assessment of the current military situation in the East from the Potomac Foundation.[21] These reports provide evidence of Russian involvement in Ukraine despite Putin's continued assertion that there are no Russian operations in Ukraine and thus Russia is not in violation of the Minsk II ceasefire agreement.[22]

Academia has also played a vital role in shaping the conversation and deepening the understanding of the causes and solutions to the war. Since the Revolution of Dignity began in late 2013, Washington D.C.-based universities have extensively provided students and the public with scholarly panels and publications from the West's misunderstanding of color revolutions to covering Ukraine's other war, rife with graft and corruption. In March 2015, George Washington University (GWU) hosted Ukrainian musician and EuroMaidan activist Sergei Fomenko. Fomenko and his band "Mandry" played several traditional Ukrainian folk songs at the opening of their exhibit titled "Ukraine. Road to Freedom," which brought the reality of the extreme measures Ukrainians took to change the status quo and avoid a dystopian future for their country to the students and public of Washington D.C. Forums and panels such as these continue to shine light on the war in Ukraine, which vacillates in and out of

[19] Ilya Iashin and Olga Shorina, *Putin. War. An Independent Expert Report* (Moscow, 2015), http://4freerussia.org/putin.war/Putin.War-Eng.pdf (accessed 30 June 2015).

[20] Pavel Felgenhauer, "Nemtsov Report on Russian War in Ukraine Fails to Have Much Impact in Moscow," *Fortuna's Corner*, 14 May 2015, http://fortunascorner.com/2015/05/14/nemtsov-report-on-russian-war-in-ukraine-fails-to-have-much-impact-in-moscow/ (accessed 30 June).

[21] Phillip A. Karber, "Russia's Hybrid War Campaign," presentation at the CSIS Russian and Eurasia Program, 10 March 2015, available at http://csis.org/event/russias-hybrid-war-campaign-implications-ukraine-and-beyond (accessed 11 March 2015).

[22] Pamela Engel, "Putin: I will say this clearly: There are no Russian troops in Ukraine," *Business Insider*, 16 April 2015, http://www.businessinsider.com/putin-i-will-say-this-clearly-there-are-no-russian-troops-in-ukraine-2015-4 (accessed 30 June 2015).

public attention given the amount of coverage devoted to other major issues such as ISIS, the refugee crisis, and a possible British exit from the EU.

Academia also has provided valuable research and analysis resources in order to achieve greater understanding of the hopes and aspirations of the Ukrainian people, who often get overlooked as geopolitical differences take precedence. The University of Maryland's Program for Public Consultation along with the Kyiv International Institute of Sociology conducted a survey of Ukrainians in all regions (except Crimea) in order to insert to the voice of Ukrainians into public knowledge and discourse.[23] The importance of understanding their opinions cannot be overstated, as various commentators and experts offer solutions to the current impasse between the Donbas region and the rest of Ukraine. A long-term and viable solution will have to take into consideration the University of Maryland's and Kyiv International Institute of Sociology's report.

## Religious Groups

Current tensions between the Moscow Patriarchate of the Russian Orthodox Church (ROC MP) and the Ukrainian Orthodox Church of the Kyivan Patriarchate began in 2009. The leader of the ROC MP, Patriarch Kirill, gave spiritual support to Putin's "Russian World" ideology. These religious tensions have created confusion on the ground as competing and radical views create an atmosphere of distrust and instability.[24] The ROC MP has played a significant role in supporting the Kremlin's narrative by articulating Russia's historical and religious links to Kyiv and Crimea.[25] According to Adrian Karatnycky of the Atlantic Council, religious leaders "are creating a deep crisis, precisely because the church was instrumentalized by these major political actors."[26] The cultural, historical and religious project known as *Novorossiya* received strong support from the Russian Orthodox Church (ROC), as it was seen "as an existential issue for the entire Holy Russia." However, the more ROC MP continues to support Russian aggression in Ukraine, the more it isolates itself now and for the future.[27]

Kirill appeals to international bodies for support of the plight of Russian Orthodox priests in eastern Ukraine, but at the same time promotes violence to-

[23] Steven Kull, *The Ukrainian People on the Current Crisis* (University of Maryland and Kyiv International Institute of Sociology, 2015), http://www.public-consultation.org/studies/Ukraine_0315.pdf (accessed 9 March 2015).

[24] Hannah Gais, "Putin's War Has Come to the Pews," *U.S. News*, 4 March 2015, http://www.usnews.com/opinion/blogs/world-report/2015/03/04/ukraine-crisis-threatens-to-further-fracture-orthodox-faithful (accessed 1 July 2015).

[25] Katya Kumkova, "Orthodox Church Leader Reflects on the Religious Dimension of the Ukrainian Crisis," *Eurasianet*, 23 January 2015, http://www.eurasianet.org/node/71756 (accessed 1 July 2015).

[26] Gais,"Putin's War."

[27] Lough, *et al.*, *Russian Influence Abroad*, 6.

ward non-Russian Orthodox religious leaders. The ROC MP's view is that the rest of the world is evil and Russia is the example of good. Russian citizens, soldiers and mercenaries have been heeding the ROC MP's de facto call to defend against the threats to the Holy Russian Empire, which is a major recruitment tactic.[28] The religious war created by the ROC MP and Kremlin stokes greater hatred and deepens the commitment by Russian fighters in Ukraine, ultimately perpetuating the rifts within society.

Any short-term gains the Kremlin is trying to make by stirring religious conflict in Ukraine with help from the ROC MP will have greater long-term ramifications for the ROC internationally.[29] The ROC MP's actions and controversial statements of its leader are creating a schism between the Ukrainian Orthodox Church, which falls under the MP, and the Ukrainian Orthodox Church of Kyivan Patriarchate. Worshippers are increasingly associating the Ukrainian Orthodox Church MP with Kremlin policies. These political differences are playing out in the pews, as 30 formerly Moscow-aligned parishes have thrown their allegiance behind the Kyivan Patriarchate. Like Kirill, leaders in the Kyivan Patriarchate make nationalistic statements such as former spokesperson Archpriest Heorhiy, who said the Moscow Patriarchate was "the Church of the Soviet Union."[30] The failure of leaders in the Orthodox Church to refrain from deep involvement in the current war is undermining the social fabric of Ukraine.

Meanwhile, non-Russian Orthodox faiths have lived in constant fear and persecution, including the Ukrainian Orthodox Churches. In June 2014, pro-Russian separatists kidnapped and murdered four Pentecostal Church leaders in eastern Ukraine. Multi-faith religious leaders from Ukraine recently met at a conference in London and called on the international religious community and NGOs to support reconciliation and peace in Ukraine. They also asked world leaders to address the humanitarian crisis of 1.2 million internally displaced persons in Ukraine.[31] Further, a damning report on religious freedoms in Russia, occupied Crimea and eastern Ukraine by the United States Commission on International Religious Freedom (USCIRF) classifies Russia as a Tier II country for freedom of religion.[32] Russian policies and actions have contributed to this ranking as well, as has a 4,000-strong Russian Orthodox Army (ROA) operating

[28] Paul Goble, "Moscow Patriarchate's Backing of Russian Aggression Undermining Russian Orthodox Church Everywhere," *The Interpreter*, 25 August 2014, www.interpretermag.com/moscow-patriarchates-backing-of-russian-aggression-undermining-russian-orthodox-church-everywhere/ (accessed 30 June 2015).

[29] Ibid.

[30] Maksym Bugriy, "The War and the Orthodox Churches in Ukraine," *Eurasia Daily Monitor*, 18 February 2015, www.jamestown.org/programs/edm/single/?tx_ttnews[tt_news]=43548&cHash=3dc1a85482a515406a43403429694d66 (accessed 1 July 2015).

[31] Ibid.

[32] Katrina Lantos Swett *et al.*, Annual Report 2015 of the U.S. Commission on International Religious Freedom (Washington, D.C.: USCIRF, 2016), p. 5.

in eastern Ukraine, which conducts destructive operations against non-Russian Orthodox religious institutions.[33]

The Ukrainian Orthodox Church played a proactive role in supporting protestors during EuroMaidan by providing church facilities for anti-government military groups.[34] Patriarch Filaret, the leader of the Kyivan Patriarchate, supports soldiers going to war in eastern Ukraine. Early this year he was in Washington DC, lobbying for military assistance to support the Ukrainian armed forces in order to defend the Ukrainian nation. Once the war broke out, the Church provided religious support and donations of money, clothes, food and transportation. According to Filaret, the Church has also provided the military with night-vision goggles.[35]

As a non-state actor, the Orthodox Church has the potential to play a constructive role by bridging the schisms in society, but until now both sides have only decreased the possibility of reconciliation between Ukrainians. The Orthodox Church has thus become a symbol of nationalism to both sides. Until the leadership of the ROC MP and Ukrainian Orthodox Church of the Kyivan Patriarchate decide that delving into the affairs of government is detrimental to society, they will continue to perpetuate the current war.

## Organized Crime

The idea of the separatist's breakaway region as "The People's Republics" of the Donbas has been years in the making. As Russia remains a mafia-like state, it benefits from having weaker, smaller countries in its periphery. Princeton historian Stephen Kotkin coined the term "Trashcanistan" to describe the pervasive nature of corruption in many of the post-Soviet countries. Through the "transition" from Communism to capitalism, many organized crime bosses became oligarchs overnight, and some rose to be powerful politicians, prime ministers and presidents. In Ukraine in particular there has been a continuous line of political leaders who rose to power through nefarious means at the cost of the development of society.[36]

The Donbas region was the most corrupt and ungovernable region by far for either Moscow or Kyiv. As the locals say, "every third man in the Donetsk region is in prison, has been in prison, or will be in prison."[37] In this paradigm,

[33] Timothy C. Morgan, "Violence, Persecution Spread in Eastern Ukraine," *Christianity Today*, 6 May 2015, www.christianitytoday.com/gleanings/2015/may/violence-persecution-spread-in-eastern-ukraine.html (accessed 1 July 2015).

[34] Lough, *et al.*, *Russian Influence Abroad*, 7.

[35] Kumkova, "Orthodox Church Leader."

[36] Mark Galeotti, "How the Invasion of Ukraine Is Shaking Up the Global Crime Scene," *Vice News*, 6 November 2014, www.vice.com/read/how-the-invasion-of-ukraine-is-shaking-up-the-global-crime-scene-1106 (accessed 1 July 2015).

[37] Piotr Kosicki and Oksana Nesterenko, "Eastern Ukraine Has Been a Mafia State for Years. Can Kiev Break the Cycle of Violence?" *New Republic*, 5 June 2014,

society does not progress and future generations are robbed of a better life. Moreover, these same individuals have openly pledged support to Russia and the separatists while claiming the Kyiv government illegally overthrew a democratically-elected Yanukovych government.[38]

The annexation of Crimea has opened a whole new market for organized crime and black market activities. Just as Transnistria, the breakaway pro-Russian enclave in Moldova, has proved profitable for Russian gangsters, Crimea has much more potential. International law enforcement organizations note that the destabilization in Ukraine has sent ripples around the world in terms of organized crime. As in Russia, Ukrainian political elite and organized crime networks are intertwined and reliant on each other for mutual support. Russian organized criminal networks are looking to expand smuggling routes using the Crimean port of Sevastopol and the prime smuggling port, Odessa. They move contraband including stolen cars, drugs, weapons and women throughout the Black Sea region.[39]

In 2014, Transparency International ranked Ukraine 142 out of 177 countries in the Corruption Perception Index. While Russia and Ukraine are in a desperate war for control of the Donbas region, Ukrainian underworld networks are collaborating with Russian ones to grow business opportunities out of the current situation in Ukraine. Moscow does not even need to engage Ukraine in a war, but simply rob Ukrainian society through Russian-Ukrainian organized criminal networks and links to corrupt officials. Russia's most dominant organized criminal organization is the Solntsevo network with strong ties to the "Donetsk clan," from which former Yanukovych's power base, the Party of Regions, stemmed. These former underground thugs are now actively serving in separatist units or attacking Ukrainian supporters and spreading terror through acts of violence.[40]

The conflict has ended any cross-border law enforcement cooperation between Russia and Ukraine, and organized crime networks are heating up in the absence of effective law enforcement networks. The "black hole" that Ukraine offers organized criminal networks within a modern state with infrastructure and ports is immense and lucrative. Thus, one of Russia's most effective responses to sanctions could be the "criminalization" of Ukraine and making it into a true "Trashcanistan."[41]

As the war rages on, organized criminal networks flourish and profit from the plight of internally displaced persons, the demands of war and the brave soldiers who fight and die for what the "Heavenly Hundred" in EuroMaidan

http://www.newrepublic.com/article/118010/eastern-ukraine-mafia-state-can-kiev-impose-rule-law (accessed 1 July 2015).

[38] Ibid.

[39] Galeotti, "Invasion of Ukraine."

[40] Mark Galeotti, "Ukraine's Mob War," *Foreign Policy*, 1 May 2014, http://foreignpolicy.com/2014/05/01/ukraines-mob-war/ (accessed 1 July 2015).

[41] Galeotti, "Invasion of Ukraine."

sacrificed their lives: a brighter future for Ukraine without corruption robbing society and future generations.

## Militias

The maligned system of politics and armed groups in Ukraine is not a new phenomenon, but a product of the Russian mafia state following the fall of the Soviet Union. As the debate over Ukraine's integration into either Europe or Russia intensified, politicians and oligarchs aligned with armed groups or created their own private armies in order to protect their interests.[42] Estimates put the number of the pro-Ukrainian volunteer militias at about 30 groups, the most prominent of which are the Azov Battalion, Dnipro Battalion and the Donbas Battalion. When war broke out in early 2014, these groups confronted pro-Russian separatists in the absence of Ukrainian armed forces.[43]

The Right Sector played a pivotal role in defending EuroMaidan activists against the pro-Yanukovych police force that attempted to break up the protestors, and has been credited with playing an important part in fighting in eastern Ukraine. The Right Sector has since gained political representation in the Ukrainian parliament, where it holds one seat.[44] Despite the organization's support for EuroMaidan and its combat role, the Right Sector is still entrenched in "old ways" of doing business, such as extortion and smuggling, which undermine its political and nationalistic platform.[45] Other militias that took part in overthrowing Yanukovych have been integrated into Ukraine's National Guard.[46]

Perhaps the most revered militia unit from the start has been the Donbas Battalion, which was originally made up of fighters from Donbas who wanted to keep Ukraine unified. Now the unit consists of volunteers from all over Ukraine and other countries. At one point, Ukrainian-American Mark Paslawsky fought in the Donbas Battalion until he was killed in a botched operation in eastern Ukraine. Paslawsky, a West Point graduate, had served as an elite ranger in the US military. Before his death, he warned of a "Maidan 3.0,"

[42] Amanda Taub, "Pro-Kiev Militias Are Fighting Putin, but Has Ukraine Created a Monster It Can't Control?" *Vox*, 20 February 2015, http://www.vox.com/2015/2/20/8072643/ukraine-volunteer-battalion-danger (accessed 1 July 2015).

[43] Ibid.

[44] "The Hand That Feeds: Kiev Now Unable to Survive without Extremist Support," *Sputnik*, 1 July 2015, http://sputniknews.com/europe/20150701/1024081705.html (accessed 1 July 2015).

[45] John E. Herbst, "Here's How to Make Sense of the Violence in Western Ukraine: Follow the Money," *Atlantic Council*, 14 July 2015.

[46] Laetitia Peron, "US Army Walks Cultural Minefield Training Ukraine Troops," *Yahoo News*, 24 April 2015, http://news.yahoo.com/us-army-walks-cultural-minefield-training-ukraine-troops-151608593.html (accessed 1 July 2015).

whereby after the war, militias that worked together would grow tired of the lack of reforms in Kyiv and continued systemic corruption.[47]

Donbas Battalion Commander Semen Semenchenko said, "We aren't anybody's army, and we don't have a single sponsor. We have many sponsors, including just ordinary people who give us as little as food and water supplies," and although last year the battalion has operated under the control of the Ministry of Internal Affairs, it still maintains some autonomy to conduct training and equipping using its own funds.[48] Semenchenko visited Washington in September 2014 to lobby on behalf of his men to receive greater US support. He will also be running for parliament in the upcoming elections, and has said "I want to make Ukraine into another Israel. I mean, a country that has seen the type of danger [Israel] has [sic] must drastically change its approach to national security and create a modern military with Special Forces to protect itself."[49]

Kyiv officials walk a thin line of outwardly condemning illegal armed groups in Ukraine and passively supporting pro-Ukrainian militias that wield significant power and fighting forces. The Ukrainian government continues to work to unify these groups under either the Ministry of Defense or Interior, despite recent confrontations and lack of desire to integrate.[50] In April 2015, the Right Sector's leader, Dmytro Yarosh, was appointed as an advisor to the Ministry of Defense in a move to consolidate the group within the ministry by giving it a seat at the table. Ultimately, officials hope that integrating all militias under the command and control of the government will achieve unity of effort against a common enemy – Russia.[51] These groups are credited with seeing EuroMaidan through to the end and defending Ukraine in the face of Russian aggression; however, as the war goes on they represent a glaring threat to the central government.[52]

[47] Simon Ostrovsky, "The Only American Fighting for Ukraine Dies in Battle," *Vice News*, 20 August 2014, https://news.vice.com/article/the-only-american-fighting-for-ukraine-dies-in-battle (accessed 1 July 2015).

[48] Sabra Ayres, "The Donbass Battalion prepares to save Ukraine from separatists," *Al Jazeera America*, 29 June 2014, http://america.aljazeera.com/articles/2014/6/28/the-donbas-battalionpreparestosaveukrainefromseparatists.html (accessed 1 July 2015).

[49] Mark Snowiss, "Q&A: Ukraine's Donbas Battalion Commander Seeks US Support," *Voice of America*, 16 September 2014, http://www.voanews.com/content/ukraine-donbas-battalion-commander-seeks-us-support/2452051.html (accessed 1 July 2015).

[50] "Ukrainian Militias Are above the Law According to Kiev," *Global Research*, 3 May 2015, http://www.globalresearch.ca/ukrainian-militias-are-above-the-law-according-to-kiev/5447023 (accessed 1 July 2015).

[51] Claire Rosemberg, "Ukraine far-right leader made army advisor in move to control militias," *Business In*sider, 6 April 2015, http://www.businessinsider.com/afp-ukraine-far-right-leader-made-army-advisor-in-move-to-control-militias-2015-4 (accessed 1 July 2015).

[52] Taub, "Pro-Kiev militias."

Pro-Russian separatist militias are known opportunists from backgrounds as organized criminals, mercenaries, Cossacks or Chechens.[53] They have been operating since the annexation of Crimea, seizing government buildings and throwing out local government administrators and law enforcement.[54] Recruitment is not only limited to eastern Ukraine, as recruitment centers have been established throughout Russia. Separatists as well as pro-Ukraine militias use Facebook or VKontakte for recruitment and organization.[55] Putin may not have direct control over these groups, and if he did want to abruptly end the war, it may have become impossible to put the lid back on the chaotic situation. Russia could be faced with the same problem as Ukraine, namely of returning fighters being dissatisfied with the conduct of the war by the Kremlin and wanting to take action in their own hands. Many right-wing groups are angry with Putin for not fulfilling the *Novorossiya* project and providing greater support for the war effort.[56]

There is concern that the worst is yet to come in eastern Ukraine. As more men receive military training and the region becomes flooded with weapons, it could lead to greater violence. As of now militias are aligned with Moscow or Kyiv, but when a political resolution is reached or one side comes out victorious, the militias will need to decide to disband or fight for personal interests. Militias on both sides are conducting their own operations and fighting and winning against government forces, showing that they will be a force to be reckoned with in the future.[57]

The most dangerous scenario is the proliferation of highly destructive weapons to disjointed militias lacking tight command and control. The shooting down of flight MH17 with a Russian-designed SA-11 antiaircraft missile demonstrates the reality of non-state actors acquiring highly sophisticated weapons systems, thus posing a direct threat to the international community.

[53] Paul Stronski, “Broken Ukraine,” *Foreign Affairs*, 18 March 2015, also available at http://carnegie-mec.org/2015/03/18/broken-ukraine (accessed 1 July 2015).

[54] Alison Smale and Andrew Roth, “Ukraine Says That Militants Won the East,” *The New York Times*, 30 April 2014, http://www.nytimes.com/2014/05/01/world/europe/ukraine.html (accessed 1 July 2015).

[55] Sarah Kaufman and Vladi Vovcuk, “Are the Russians Losing Interest in Ukraine?” *The Week*, 13 June 2015, http://theweek.com/articles/560117/are-russians-losing-interest-ukraine (accessed 1 July 2015).

[56] Stronski, “Broken Ukraine.”

[57] Stephen Biddle and Ivan Oelrich, ”Why the Ukraine Separatists Screwed Up: Badly Organized Insurgents Can’t Master Complex Weapons Systems,” *The Washington Post*, 21 July 2014, www.washingtonpost.com/blogs/monkey-cage/wp/2014/07/21/why-the-ukraine-separatists-screwed-up-badly-organized-insurgents-cant-master-complex-weapons-systems/ (accessed 18 July 2015).

## NGOs and GONGOs

Throughout the 2000s, Putin observed the power of Western democratic NGOs throughout the former Soviet Union and has now begun countering their democratization objectives with Russian NGOs. Russia's objectives are to promote the "Russian" model, seek to reduce influence of the US and once again become the center of gravity for the region. When Putin returned to power he set about nationalizing Russian civil society, namely pro-Russian think tanks, human rights groups, election observers, youth groups, Eurasianist integration groups and Cossack networks. All of these organizations have been heavily involved in weakening Ukraine: some were used to counter the Revolution of Dignity, support the annexation of Crimea and to undermine sovereignty and stir social tensions throughout Ukraine.[58]

Beyond the borders of the former Soviet Union, Russia supports about 150 GONGOs with the goal of influencing policymakers, political elite and youth. Compared to Western lobbyist organizations that rely on the strength of their argument, Russians see money as the most influential tool of persuasion. The development of business links in Germany, Italy and France has been influential in Europe's lackluster response to Russia's actions in Ukraine. Moreover, Europe and the US have taken military intervention off the table, which has greatly undermined the negotiating strength of the international community.[59] These operations have had a direct impact on the war in Ukraine by creating opposition in the West to Russian sanctions, military intervention and the international community's ability to speak with one voice to condemn Russian aggression.

During the annexation of Crimea, the Cooperation Agency, the Luzhkov Sevastopol Foundation and the Moscow House of Crimea funded the separatist leadership. Sergey Tsekov, a Crimean Russian separatist leader, has run the youth movement in Crimea since 2008. Through his organization he promoted Russian values and interests by organizing demonstrations against NATO, pro-Russian performances and promoting reunification with Russia. The *Novorossiya* project was also strongly supported by Russian GONGOs with religious undertones. The Izborskiy Club, for instance, was instrumental in organizing a new government in eastern Ukraine and the St. Basil's Foundation cooperates with the new "Donetsk People's Republic" (DNR) by providing aid to the war-torn region. Several recruitment organizations such as Russian Volunteers, the Russian Imperial Movement and Veterans and Cossacks have fed the meat grinder in Ukraine with fresh ideological Russians.[60]

In the past, Western NGOs enjoyed the advantage of an open society and massive funding in the former Soviet space. To counter the influence of these NGOs, Russia has used GONGOs to promote Russian values. GONGOs have lost

[58] Lough, *et al.*, *Russian Influence Abroad*.

[59] Ibid.

[60] Ibid.

their appeal as international opinion of Russia is increasingly negative as the conflict in eastern Ukraine drags on into its second year. Their narrative of a Eurasian community with Russia as the center of gravity is becoming less appealing to their target audiences throughout the former Soviet space, and especially in Ukraine.[61]

Ukrainian civil society has been the most active within the former Soviet space. The National Endowment for Democracy (NED) has been instrumental in providing funding, and currently sponsors more than 80 NGOs in Ukraine that work in areas such as supporting civil society's participation in government, strengthening public sector transparency and media development. For example, the Independent Association of Broadcasters works with youth to develop bipartisan video segments comparing various political parties' platforms.[62] NED's support for strengthening NGOs and societal inclusion may have contributed to Ukrainians deposing former president Yanukovych following mass protest in Kyiv. The appeal of an open and inclusive society more integrated with the greater European neighborhood proved superior to continued subservience to Russia.

Also present in Ukraine, humanitarian NGOs inject themselves into events by reporting on prisoner of war abuses and war crimes as well as working with internally displaced persons. Amnesty International released a report in May called *Breaking bodies: Torture and Summary Killings in Eastern Ukraine* on prisoner abuse after interviewing 33 former prisoners, half from the Ukrainian side and half from the separatist/Russian side. According to their account, prisoners were "beaten until their bones broke, tortured with electric shocks, kicked, stabbed, and hung from the ceiling, deprived of sleep for days, threatened with death, denied medical care, and subjected to mock executions."[63]

Pro-Russian and pro-Western civil NGOs and GONGOs are actively pursuing conflicting goals in Ukraine. Over time, the natural desires of Ukrainian civil society to shed corruption and reject the model of the Russian mafia state have exploded in uprisings of society against elite politicians whose loyalty to Moscow supersede the will of Ukrainians.

## Diasporas

Since 1940, the interests of the 961,100 Ukrainians in the US have been represented by the Ukrainian Congress Committee of America, Inc. (UCCA).[64] Its pub-

[61] Ibid.

[62] National Endowment for Democracy, www.ned.org/where-we-work/eurasia/ukraine (accessed 19 July 2015).

[63] Amnesty International, *Breaking Bodies: Torture and Summary Killings in Eastern Ukraine* (London: Amnesty International, 2015), http://www.amnestyusa.org/sites/default/files/ukraine_briefing_final.pdf (accessed 30 June 2015).

[64] Olena Lennon, "Ukrainian Politics Abroad," *Foreign Affairs*, 17 March 2015, www.foreignaffairs.com/articles/eastern-europe-caucasus/2015-03-17/ukrainian-politics-abroad (accessed 30 June 2015).

lic relations office, the Ukrainian National Information Service (UNIS), located in Washington, is very active. Since the Revolution of Dignity began in late 2013, the UCCA and UNIS have been working to raise the issues of Russian aggression, preserving Ukraine's territorial integrity and greater US support for Ukraine during the ongoing war. The UNIS organizes advocacy days in Washington and works closely with the newly-formed Senate Ukraine Caucus to discuss policy measures that will strengthen the strategic relationship between the US and Ukraine, especially to deter further Russian aggression. UCCA's reputation and credibility has strengthened government and business contacts during the difficult period of war and necessary reforms have thus been enacted by the government.[65]

Representatives from Ukraine have also made a continuous effort to engage the Ukrainian diaspora in the US. Early this year Ivan Rodichenko, a volunteer fighter, visited a New York Ukraine Chapter and brought US-Ukrainians a personal story and pictures from the front lines. During Rodichenko's presentation, the audience donated funds to purchase equipment and supplies for his unit. "Without this help from people like them, the war is already lost," said Rodichenko. He represents one of 32 defense battalions, each with its own spokesman who travels to various diaspora groups to raise awareness of the poorly-equipped volunteer units that receive minimal funding from Kyiv. The Ukrainian diaspora throughout the world has donated "hundreds of thousands of dollars" to Rodichenko's unit, which went to purchase basic military personnel equipment such as sleeping bags, clothing and radios.[66]

In Portugal, a country of 10 million people, the Ukrainian diaspora represents the second largest immigrant community, with 45,000 Ukrainians. According to the Ukrainian World Congress, almost one-third of Ukrainians live outside Ukraine. Thus, diaspora support is vital in the face of Russian aggression and will be instrumental in rebuilding the country and paying of its foreign debt in the future. For Ukraine—one of Europe's poorest countries—remittances make up 5 percent of GDP. During the Revolution of Dignity in Euro-Maidan, Ukrainians in Portugal raised $55,000 for the demonstrators.[67] Canada also has a large and active Ukrainian diaspora, which over the past year has raised between $10-15 million.[68]

[65] www.ucca.org/index.php?option=com_content&view=article&id=13&Itemid=10&lang=en.

[66] Christopher Harress, "How the Ukrainian Diaspora in the US Is Funding the War Effort in East Ukraine," *International Business Times*, 15 March 2015, http://www.ibtimes.com/how-ukrainian-diaspora-us-funding-war-effort-east-ukraine-1846674 (accessed 30 June 2015).

[67] Paul Ames, "Ukraine's Diaspora Could Be Key to Recovery," *Global Post*, 22 May 2014, www.globalpost.com/dispatch/news/regions/europe/140301/ukrainian-diaspora-ukraine-economic-recovery (accessed 30 June2015).

[68] Ibid.

The Ukrainian diaspora has mobilized itself financially, technically and personally, fighting on the front lines to come to the aid of its countrymen. Grassroots efforts supply both the volunteer units and government forces with over half of what they need, making the diaspora a powerful actor. This is a more efficient and transparent process compared to an improving, yet still corrupt, poorly funded and dysfunctional defense system.[69]

Furthermore, diasporas do have an effect on political leaders, especially in Canada, where Steven Harper was ranked within the top 10 "most influential promoters of Ukrainian issues in the world."[70] The Ukrainian diaspora has also proven to be a powerful force in supporting Ukraine's move toward greater independence and democratization. From humanitarian aid to wounded soldiers receiving the highest level of care in other countries, the Ukrainian diaspora is providing funding where the government in Kyiv cannot.[71] Outside of the UCCA, the *Razom for Ukraine* group unites highly skilled professionals in the Ukrainian diaspora inside and outside the US, and has raised around $135,000 for the Maidan protests.[72]

## Conclusion

The current situation in Ukraine has highlighted the fact that in this new age of warfare, non-state actors play a larger role than ever before. They greatly impacted the root causes leading up to the Revolution of Dignity, the annexation of Crimea and the prolonged war in eastern Ukraine. Russia has found it necessary to employ a myriad of traditional non-state tools to protect its strategic interests in Ukraine. In Kyiv, the Ukrainian government is dealing with an economic crisis and fighting a war for its very survival, but must also take into consideration interests of non-state actors. Leaders who understand the influence of these groups, sources of funding and motivation will be more able to navigate this complex environment, where one misinformed decision could lead to negative consequences and prolonged suffering. The twenty-first century battlefield in Ukraine is complex and characterized by the active participation of non-state actors, creating a hotbed for hate and deadly struggle over geostrategic, economic and security interests. The conclusion of the war will hinge upon the ability of either side to capitalize on the influence non-state actors wield not only in Ukraine, but transnationally.

[69] Ibid.

[70] Mark Mackinnon, "Bypassing Official Channels, Canada's Ukrainian Diaspora Finances and Fights a War against Russia," *The Globe and Mail*, 26 February 2015, http://www.theglobeandmail.com/news/world/ukraine-canadas-unofficial-war/article23208129/ (accessed 30 June 2015).

[71] Lennon, "Ukrainian Politics Abroad."

[72] Katya Soldak, "In a Time of Crisis, Ukrainians Abroad Unite," *Forbes*, 10 April 2014, www.forbes.com/sites/katyasoldak/2014/04/10/in-a-time-of-crisis-ukrainians-abroad-unite/ (accessed 30 June 2015).

## About the author

MAJ Joshua Mulford is from Centreville, Virginia. In 2004 he graduated from Virginia Military Institute and commissioned as a Second Lieutenant in the U.S. Army Infantry. Joshua deployed twice to Iraq and has served throughout the former Soviet Union. Joshua has completed his Masters in International Policy and Practice with a Concentration in Eurasian Affairs from George Washington University, Washington D.C. He is currently attending the Joint Military Attaché School and is the Deputy Attaché (designate) to the U.S. Embassy Yerevan. MAJ Mulford is married to Sohira; they have two daughters, Anais and Laurel.
E-mail: jpmulford@gwmail.gwu.edu

*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Oliver Fitton, *Connections QJ* 15, no. 2 (2016): 109-119
http://dx.doi.org/10.11610/Connections.15.2.08

**Research Article**

# Cyber Operations and Gray Zones: Challenges for NATO

*Oliver Fitton*

*Politics, Philosophy & Religion Department, Lancaster University, http://www.lancaster.ac.uk/*

**Abstract**: The Gray Zone represents a space between peaceful state rivalries and war. Within this space actors have developed hybrid strategies to extend their influence. This concept of conflict is best illustrated by Russia's actions in Eastern Ukraine in 2014. Gray Zone doctrine leverages ambiguity to create an environment in which adversaries are unable to make strategic decisions in a timely and confident manner. Cyber Operations, because of the attribution problem, lend themselves to this kind of conflict. This article explores the interactions between the Gray Zone and cyber operations and considers questions which NATO must address in order to adapt.

**Keywords**: cyber war, gray zone, ambiguity, NATO, hybrid war.

## Introduction

Russia's annexation of Crimea in 2014 represented a severe challenge to NATO. The events that took place in Eastern Ukraine involved a hybrid strategy, which relied heavily on ambiguity. Strategists in Moscow used conventional forces, a grip on Russian-language media, a loose interpretation of international law, local proxies, information operations and cyber operations as tools to operate within the gray zone between war and peace. Although what Russia achieved in Crimea represented more than peaceful competition between states, it was achieved without triggering a large-scale military engagement.

In 2007 Russia launched another gray zone operation that navigated the fine line between war and peace. The denial of service attack that crippled Estonia in April of that year was the result of tensions between the two countries boiling over. Russia did not employ an armed response, which would inevitably invoke Article 5 of the North Atlantic Treaty. Instead, a new kind of deniable operation was used, which lent itself to the gray zone: a cyber operation.

It is argued throughout this article that cyber operations have and will continue to be an effective tool for the adversaries of NATO as part of a gray zone strategy. The nascent concept of the gray zone will be explored and its relationship with hybrid warfare elucidated. The applicability of cyber operations to gray zone strategy will be discussed in terms of the problem of attribution for the victim and the advantage deniability affords for the attacker. Finally, three challenges NATO faces as a result of cyber operations within the gray zone will be presented. Firstly, the challenge ambiguity represents to Article 5 of the North Atlantic Treaty; secondly, achieving deterrence against limited operations that erode NATO influence; and finally, how to navigate this new norm of conflict that liberal democratic principles prohibit. It is beyond the remit of this article to solve these problems; the objective is rather to compel the academic community to engage with the challenges of the gray zone and how cyber operations will be assimilated into future strategies.

## The Gray Zone

The gray zone between war and peace is the primary characteristic of modern conflicts. Carl von Clausewitz considers war to be an extension of a duel between two parties, "an act of violence intended to compel our opponent to fulfil our will."[1] For the majority of human history this definition of war was self-evident. From the Peloponnesian War onwards a state of war involved a known adversary with clear political objectives in opposition to one's own. According to General Curtis LeMay, winning wars was simple: "You've got to kill people and when you kill enough of them, they stop fighting."[2] Clausewitz's definition of war imbues with unchanging characteristics – war is violent, instrumental and political.[3] However, recent attention in academia and policymaking (especially within NATO) to concepts including hybrid wars, ambiguous wars and limited wars suggests that the character of war is changing – or at least the threats the Alliance faces are becoming less easily defined.

Of the scholars from multiple disciplines who have engaged with the concept of hybrid warfare over the years,[4] Frank Hoffman is perhaps the most widely quoted. According to his definition, hybrid warfare is a deviation from

[1] Carl von Clausewitz, *On War*, ed. Anatol Rapoport (Harmondsworth: Penguin Books, 1982), 101.

[2] Richard Rhodes, *The Making of the Atomic Bomb* (London: Simon & Schuster, 2012), 586.

[3] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

[4] See e.g. Larry R. Jordan, *Hybrid War: Is the US Army Ready for the Face of 21st Century Warfare*, Master's thesis (US Army Command and General Staff College, 2008); Mackubin Thomas Owens, "Reflection on Future War," *Naval War College Review* 61:3 (2008): 61–76; and Russell W. Glenn, *All Glory Is Fleeting: Insights from the Second Lebanon War* (Santa Monica, CA: RAND, 2012).

previous incarnations: "Instead of separate challenges with fundamentally different approaches (conventional, irregular, terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously."[5] The paragon of such doctrine for Hoffman was Hezbollah in the 2006 Second Lebanon War, during which Hezbollah repelled a vastly superior Israeli conventional force through the use of both conventional and unconventional tactics.[6] Following Hoffman's interpretation of hybrid threats, the United States (US) will more frequently contend with adversaries capable of employing conventional weapons such as anti-tank and cruise missiles and unmanned aerial vehicles, while using irregular tactics such as hiding among the civilian population and improvised explosive devices. There is limited literature on cyber operations and their significance within hybrid strategies.[7] However, there is a much greater discussion surrounding the concept of cyber war as a distinct concept that is highly pertinent to the subject of hybrid war and gray zone conflict.[8]

Gray zone conflict and hybrid war are not interchangeable concepts. Indeed, the use of the term "conflict" for the former and "war" for the latter is deliberate. The use of "unconventional" and "irregular" tactics is not limited to the strict Clausewitzian paradigm of war. The concept of the gray zone seeks to encompass operations that fall short of warfare due to intensity, legality or (most interestingly) ambiguity. Unconventional tactics can involve information, psychological, diplomatic or economic operations outside the definition of "warfare" if it is to be used in any meaningful sense. NATO commanders have begun to publically express concern over such unconventional threats.[9] It is the extensive use of unconventional tactics outside of strictly defined wartime that has contributed to a crisis in confidence within NATO.[10] US Special Operations Command is embarking upon a yearlong research project entitled *The Gray Zone*. The project aims to give the US government the tools to understand gray zone threats and create effective responses to them. The gray zone is defined

[5] Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (2009): 35.

[6] Ibid., 37.

[7] See Sascha-Dominik Bachmann and Hakan Gunneriussan, "Hybrid Wars: The 21st Century's New Threats To Global Peace And Security," *Scientia Militaria, South African Journal of Military Studies* 43:1 (2015): 77–98.

[8] See e.g. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12:2 (1993): 141–165; Richard A. Clarke, *Cyber War: The Next Threat to National Security And What To Do About It* (New York: HarperCollins, 2010); and Rid, *Cyber War Will Not Take Place*.

[9] John Vandiver, "Breedlove: NATO Must Redefine Responses to Unconventional Threats," *Stars and Stripes*, 31 July 2014, http://www.stripes.com/news/breedlove-nato-must-redefine-responses-to-unconventional-threats-1.296129 (accessed 23 January 2016).

[10] Peter Apps, "'Ambiguous Warfare' Providing NATO with New Challenges," *Reuters*, 21 August 2014, available at http://uk.reuters.com/article/uk-nato-summit-idUKKBN0GL1KA20140821 (accessed 23 January 2016).

as the region between peace and war, which is not yet fully understood. Actions undertaken in the gray zone go beyond normal peacetime competition but fall short of all-out war.[11]

Russian operations in Eastern Ukraine and Crimea had both a hybrid and ambiguous character. In 2014 Russia used a combination of conventional military forces (for example, amassing on the Russia/Ukraine boarder and naval patrols) and unconventional tactics (for example, "the little green men" and information dominance attained by leveraging Russian nationalism in East Ukraine) to secure the annexation of Crimea. These actions caused alarm throughout the Alliance despite Ukraine's status as a NATO non-member. Engineered uncertainty in Russian action and rhetoric crippled the Alliance's ability to respond and has the potential to do so again should the doctrine be employed against NATO members in Eastern Europe.[12] Whether these tactics were new or anchored with historical precedent remains a matter of debate.[13] What is clear, however, is that NATO is unprepared for gray zone conflict.

As demonstrated in Eastern Ukraine, ambiguity is a useful tool. Without a full picture of validated information, it becomes difficult for a strategist to choose the optimal course of action. By allowing ambiguity to feature within strategic decisions or by actively inserting ambiguity into strategy, it is possible to cloud the vision of enemy. The United Kingdom (UK) employs a policy of deliberate ambiguity in its strategic nuclear deterrent. As a result, adversaries of the UK are unaware of "when, how and at what scale"[14] the UK government would be willing to use nuclear weapons, including whether they would be used on a first-strike basis. A clear statement on the planned use of the nuclear deterrent would allow adversaries to more clearly calculate their own strategies. Ambiguity within strategic nuclear deterrence allows states to operate below the threshold of conflict by not explicitly threatening an individual adversary. It was a balance between known variables and ambiguous strategies that maintained stability during the Cold War.

[11] United States Special Operations Command, "The Gray Zone," White paper, 9 September 2015), 1, http://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf (accessed 23 January 2016).

[12] For further discussion on this topic see House of Commons Defence Committee, *Towards the next Defence and Security Review: Part Two – NATO* (London: House of Commons Defence Committee, 2014), and in particular the evidence given to the Committee by Sir Bob Russell.

[13] Peter R. Mansoor discusses this debate, which centers on competing definitions of "hybrid warfare," in "Hybrid Warfare in History," introductory chapter in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012).

[14] HM Government, *The Future of the United Kingdom's Nuclear Deterrent*, December 2006, Cm 6994, at 18.

Gray zone strategy is employed by non-liberal democratic states and authoritarian non-state actors. Such strategy, especially the use of ambiguity, is antithetic to societies based upon social pluralism, binding legal principles and government accountability. Accountability and transparency are especially sought after in public discourse regarding military action following the invasion of Iraq in 2003 and the publication of the infamous "dodgy dossier."[15] Such desire was palpable in the UK during the recent debates over intervention in Syria. Democratic accountability functions to limit the degree to which governments can employ ambiguity.

Russia, however, is unrestrained by social pluralism and government accountability. Dissent has been met with violence.[16] Putin's administration has a strong grip over the majority of the Russian speaking media in the region.[17] Russian decision making is dramatically less transparent than that of NATO members. Russia is therefore relatively unrestrained in its ability to employ both conventional and unconventional operations against their adversaries. Daesh represents freedom of operation to an even greater degree, owing to its disregard for international law. In a straightforward Clausewitzian scenario, war is clearly understood and established rules of engagement apply. NATO is designed to win these wars. In gray zone conflict it is not clear who the enemy is or what their intentions are, forcing liberal democracies to question the legitimacy of their responses with much greater scrutiny than non-democratic actors. Liberal democracies are greatly restrained in situations where autocratic states and non-state actors are not. This results in a strategic imbalance that threatens and undermines the strategic advantage NATO provides.

## Cyber Operations

As NATO's adversaries develop strategies to exploit the gray zone, conventional force is likely to be used in new ways and new unconventional tactics will appear. Some unconventional tactics are likely to be more effective than others. Cyber operations represent a developing unconventional approach that can be highly effective within gray zone conflict.

Cyber operations are facilitated by reliance on networked communication. They exclusively utilize computer code in order to alter, collect data from or deactivate computer systems that have software, hardware and human components. Cyber operations cannot be directly violent because computer code

[15] The poorly researched and attributed intelligence report that claimed that Iraqi weapons of mass destruction could be readied for use within 45 minutes. This dossier was employed by the Blair government to support the argument for military intervention in Iraq in 2003.

[16] For example, the death of Boris Nemtsov in February 2015 and the violent suppression of members of the music group Pussy Riot during their demonstrations at the 2014 Sochi Winter Olympics.

[17] Scott Gehlbach, "Reflections on Putin and the Media," *Post-Soviet Affairs* 26:1 (2013): 78.

cannot directly damage a human in the same way as kinetic, energy or agent-based weapons.[18] Nevertheless, they have become a notable element of modern conflict, including being used to shut down nuclear enrichment facilities[19] and spy on governments.[20] In the recent UK National Security Strategy and Strategic Defence and Security Review 2015, the government committed £1.9 billion to "protecting the UK from cyber attack and developing … sovereign capacities in cyber space."[21] Cyber operations are of particular value in gray zone conflict thanks to two key characteristics: inherent problems associated with attribution and deniability on the part of the attacker.

For adversaries who want to make strategic gains without reaching the conflict threshold laid down by NATO (Article 5), the idiom "on the Internet no one knows you're a dog" rings particularly true. Anonymity is a central characteristic of activity in cyberspace. Attributing cyber attacks to adversaries (be they individuals, non-state actors or nation states) is complex, time consuming and challenging. Furthermore, it is unlikely that the resulting verdict of attribution will be so certain as to justify a traditional military response. Therefore, the deterrence effect that NATO has been so successful in achieving in terms of armed conflict in Europe does not apply to cyber operations. Indeed, many NATO members have been struck by various forms of cyber attack, most notably the large-scale denial of service attack against Estonia in 2007.[22]

In 2015 Thomas Rid and Ben Buchanan assessed the attribution problem in an attempt to understand its challenges and advise policymakers on a potential solution. They concluded that attribution analysis is an art form requiring "skill, tools as well as organizational culture: well-run teams, capable individuals, hard-earned experiences and often and initial, hard-to-articulate feeling that 'something is wrong.'"[23] Further, they warn that attribution is not a binary matter of possible versus impossible. Rather, attribution can be achieved with varying levels of certainty. Perhaps most importantly, Rid and Buchanan point out that attribution is a matter of political will: it depends on the resources that governments want to put into tackling it.

Rid and Buchanan developed a system they call the "Q Model" for attribution. This model requires three layers of scrutiny including tactical (technical),

[18] Rid, *Cyber War Will Not Take Place*, 13.

[19] For further details on the Stuxnet incident see Nicolas Falliere, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier* (Cupertino, CA: Symantec Corporation, 2011).

[20] For further details on the GhostNet incident see "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 29 March 2009.

[21] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015, Cm 9161, at 40.

[22] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," White paper presented at the 2008 Black Hat Conference, 7.0.

[23] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015): 30.

operational and strategic analysis. At the tactical level, technicians identify that an attack has taken place and use all the tools at their disposable to understand the *how* of the attack. How did the adversary gain entry to the system and how did they create an effect after successful access? This stage of analysis may focus on tracking Internet Protocol (IP) addresses, observing the adversary's movement around the system in question, reverse engineering of malicious code and a host of other technical skills. At the operational level, the technical analysis is compiled and assessed alongside other sources of information, such as non-technical analysis (possibly signals intelligence and human intelligence), analysis of similar attacks and the wider geopolitical context to create hypotheses about what happened – the *what* of the attack. Finally, the strategic layer attempts to understand the *who* and the *why* of the attack. At this point, decision-makers consider the operational hypotheses, debate who may be responsible and formulate a response based on the attack's significance. The final aspect of the Q Model is to communicate attribution to the wider community.

However, this model does not solve the problem of attribution. Advanced adversaries will still be able to obfuscate their role in cyber operations to a certain degree, most likely by pointing the finger at another actor. This can be achieved with the use of a certain language or skillful placement of what appear to be coding mistakes. Rid and Buchanan point out that "The perfect cyber attack is as elusive as the perfect crime."[24] However, adversaries in hybrid war do not need to achieve the perfect unattributable cyber attack; they simply need to cause enough doubt in the minds of analysts to limit or slow policymaker's responses.

The second characteristic of cyber operations that is particularly important to understand in the context of hybrid strategies is deniability. There is an increasing trend towards deniable partnerships between states and cyber operations specialist groups, which insulates the state from blame for disruptive unconventional campaigns. During the early stages of the civil war in Syria, President Bashir Al-Assad's regime developed an ambiguous relationship with a group called the Syrian Electronic Army (SEA). The SEA was a pro-Assad movement that hacked into Western websites and social media accounts, defacing them and spreading pro-Assad messages. High-profile targets included the *Onion*, the Associated Press (AP) and Harvard University.[25] However, the SEA was not Assad's personal cyber army, and their relationship was often publically strained.[26] As a result, Assad could plausibly deny that his regime was responsi-

[24] Ibid., 32.

[25] For further discussion of the activities of the Syrian Electronic Army and its attacks see Oliver Fitton and Mark Lacy, "The Syrian Electronic Army Is Rewriting the Rules of War," *The Conversation*, 3 September 2013, http://theconversation.com/the-syrian-electronic-army-is-rewriting-the-rules-of-war-17618 (23 January 2016).

[26] Adam Jones, "Syrian Electronic Army Turns on Assad Regime," *Seczine: Security Magazine*, 21 August 2013, http://seczine.com/cyber-security/2013/08/syrian-electronic-army-turns-on-assad-regime/ (accessed 23 January 2016).

ble for defacing Western websites and stealing data from US institutions while benefiting from the tactical success of the SEA. It has been suggested that Russia used the very same model to carry out cyber attacks on the Georgian government in 2008 and Estonian financial institutions in 2007 through the organization known as the Russian Business Network (RBN).[27]

Cyber operations are difficult to attribute and in some cases deniable even if a degree of attribution is possible. They also have the potential to be extremely dangerous. While computer code will never kill a human being directly, it is highly likely that cyber attacks on industrial or societal infrastructure will one day result in death. For example, in 2006 the Aurora experiment demonstrated that code-based exploits can result in kinetic effects,[28] and in 2010 the Stuxnet worm proved to be behind the malfunctions of centrifuges at the Natanz nuclear facility in Iran. The potential for both ambiguity and effectiveness means that cyber operations are very likely to be employed by gray zone adversaries in the future as they have been in the recent past.

## Challenges for NATO

NATO recognizes that hybrid warfare is a strategy it must come to understand and learn to combat. NATO must take special notice of the role that cyber operations play within hybrid strategies with special emphasis on their ambiguous nature. Three specific challenges are apparent. First, there is the question of how to apply Article 5 of the North Atlantic Treaty in the case of a cyber attack on a NATO member state if attribution is not a binary proposition. Second, if attribution and deniability restrain NATO's use of force, the Alliance must find a way to deter adversaries from the use of low-intensity tactics, such as those employed in Estonia, Georgia and Eastern Ukraine. Finally, it remains to be seen whether NATO can employ cyber operations as part of a gray zone strategy while respecting the liberal democratic principles that separate the Alliance from its adversaries. In other words, it would be wise for NATO to engage in gray zone strategies.

Article 5 of the North Atlantic Treaty states that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." As such, the Alliance will take "action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[29] The first problem with Article 5 regarding cyber attacks is the debate around the degree to which cyber attacks represent an "armed

[27] Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (New York: Public Affairs, 2010), 212–213.

[28] Fortinet, "Securing SCADA Infrastructure," White paper (Sunnyvale, CA: Fortinet, 2010), 6.

[29] "The Atlantic Charter," last modified 1 October 2009, available at www.nato.int/cps/bu/natohq/official_texts_16912.htm.

attack."[30] If cyber attacks cannot be considered violent[31] there must be debate over their status as "armed attacks". If a cyber attack is not considered to be an armed attack, such an event does not automatically trigger the process of collective response on which European security has been based since the end of the Second World War. However, this view has been challenged in the wake of the 2007 cyber attacks against Estonia. NATO Secretary-General Jens Stoltenberg confirmed that NATO deems cyber attacks within the spirit of the requirements for action based upon Article 5 commitments.[32] This echoes the unilateral stance taken by the United States.[33]

The next question associated with this first challenge is how to justify a military response to a cyber attack invoking Article 5 when the process of attribution (as described by Rid and Buchanan) requires time, investment and a multilayered approach in order to produce a conclusion that is unlikely to be one hundred percent certain. Even if the legality of an armed response to a cyber attack is agreed upon, the confidence of NATO commanders in their actions must be based on the fallible science of attribution. Moreover, it will be difficult for NATO to react decisively if the adversary suspected of carrying out a cyber attack has a degree of built-in deniability, such as those between Russia and the RBN or Assad's regime in Syria and the SEA. Were cyber operations to take place alongside clear conventional military operations (as seen in Georgia in 2008), actions based on Article 5 would be clearly justified. If cyber operations were to precede the use of conventional tactics within a hybrid strategy, NATO may find itself constrained, divided and unable to act decisively as a result of an adversary engineering uncertainty through plausible deniability.

The second challenge NATO must overcome is how to deter cyber operations against NATO members. The full extent of a nation state's cyber capability is necessarily a matter of ambiguity. Should specific capabilities be revealed, the exploits upon which they are based are liable to be fixed and that capability rendered useless. This is a fundamentally different challenge compared to conventional and nuclear deterrence. While cyber operations may never be comparable to conventional or nuclear warfare to the extent that they represent an existential threat to a nation-state, it is likely that they may be used to destabilize societies, economies and populations within the sphere of influence of an adversary as part of a wider hybrid doctrine. Such destabilization may contrib-

[30] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 3.

[31] See Rid, *Cyber War Will Not Take Place.*

[32] Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," *Defense News*, 25 March 2015, available at www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930 (accessed 23 January 2016).

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, 31 May 2011, available at http://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (accessed 23 January 2016).

ute to the erosion of NATO's influence and ability to secure its strategic objectives.

The final challenge relates to how NATO's liberal democratic principles restrain it from employing the same tactics used by its adversaries, despite the opportunity to do so, and to achieve strategic success. NATO members, in particular the US and UK, have some of the largest investments in cyber operations. However, they are the nations that will be the most constrained from using such unconventional tactics openly. Liberal democratic principles including the rule of law, government accountability and transparency should restrict these states from employing their unconventional operations during peacetime. As a result, NATO is at risk of being left in a doctrinal deficit more difficult to overcome than any technology gap. NATO's adversaries are thus able to take advantage of the gray zone between war and peace: Daesh can gain territory while spreading fear and its radical message and Russia is able to make territorial and psychological gains in Eastern Europe, while NATO itself is philosophically bound to uphold strict virtues. As a result, NATO stands to have its influence eroded while being unable to play the very game it is losing.

Nevertheless, pragmatism may inevitably come before virtue. Russia has long accused the West of using the very ambiguous strategies that Western academia now recognizes Russia to be employing.[34] According to Timothy L Thomas, Russian scholars have long viewed the Soviet defeat to be the result of a clandestine information war.[35] There are question marks around how sustainable such a doctrine might be in the modern age. It is entirely possible that NATO members could create deniable relationships with online non-state actors in order to achieve the kinds of deniable partnerships that have been enjoyed by Assad and Putin. Indeed, this may be easier for liberal democratic states. The principles of many online groups often include liberty, equality and positivism, if not rule of law. However, any evidence of such partnership is likely to cause some tension between populations and governments in a post Wiki-leaks world. Furthermore, the deniability enjoyed by adversaries comes at the cost of command and control, which can lead to unintended consequences for highly networked societies. As a result, deniable partnerships are unlikely to be appealing in a NATO gray zone strategy.

## Conclusion

Gray zone conflict marks an extension of hybrid warfare into the space between war and peace. It employs both conventional and unconventional methods to achieve political goals, as well as ambiguity to cloud the judgement of adversaries. Cyber operations are an unconventional tactic that has been and

[34] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, 2009), 486.

[35] Ibid., 477.

will continue to be used in gray zone approaches by NATO’s adversaries. Issues surrounding the attribution of cyber operations and engineered deniability on the part of adversaries drastically restrain NATO’s ability to respond to cyber operations. It is vital that NATO develop a means by which to respond and deter such tactics, not only because of the damage cyber attacks might cause, but also because of their potential to erode NATO’s influence in contested spheres.

## About the author

Oliver Fitton is a PhD candidate in the Department of Politics, Philosophy and Religion at Lancaster University, UK and a researcher for Security Lancaster, a GCHQ Centre of Excellence in Cyber Security. His research focuses on cyber operations and ambiguity in modern and future conflict.
E-mail: o.fitton@lancaster.ac.uk.