**10 trends for the future of warfare**



Image: Oliver Barrett

03 Nov 2016

1. [Anja Kaspersen](https://www.weforum.org/agenda/authors/anja-kaspersen) Former Head of Geopolitics and International Security, World Economic Forum
2. [Espen Barth Eide](https://www.weforum.org/agenda/authors/espen-barth-eide) Member of Parliament, Parliament of Norway
3. [Philip Shetler-Jones](https://www.weforum.org/agenda/authors/philip-shetler-jones) Programme Lead, International Security, World Economic Forum

Latest Articles

[[](https://www.weforum.org/agenda/2018/02/podcast-your-government-needs-updating)](https://www.weforum.org/agenda/2018/02/podcast-your-government-needs-updating)

**[Podcast: Your government needs updating](https://www.weforum.org/agenda/2018/02/podcast-your-government-needs-updating)**

[Anne Marie Engtoft Larsen 20 Feb 2018](https://www.weforum.org/agenda/2018/02/podcast-your-government-needs-updating)

[[](https://www.weforum.org/agenda/2018/02/heres-what-could-buy-us-some-time-before-cape-town-runs-out-of-water)](https://www.weforum.org/agenda/2018/02/heres-what-could-buy-us-some-time-before-cape-town-runs-out-of-water)

**[Here's what could buy us some time before Cape Town runs out of water](https://www.weforum.org/agenda/2018/02/heres-what-could-buy-us-some-time-before-cape-town-runs-out-of-water)**

[20 Feb 2018](https://www.weforum.org/agenda/2018/02/heres-what-could-buy-us-some-time-before-cape-town-runs-out-of-water)

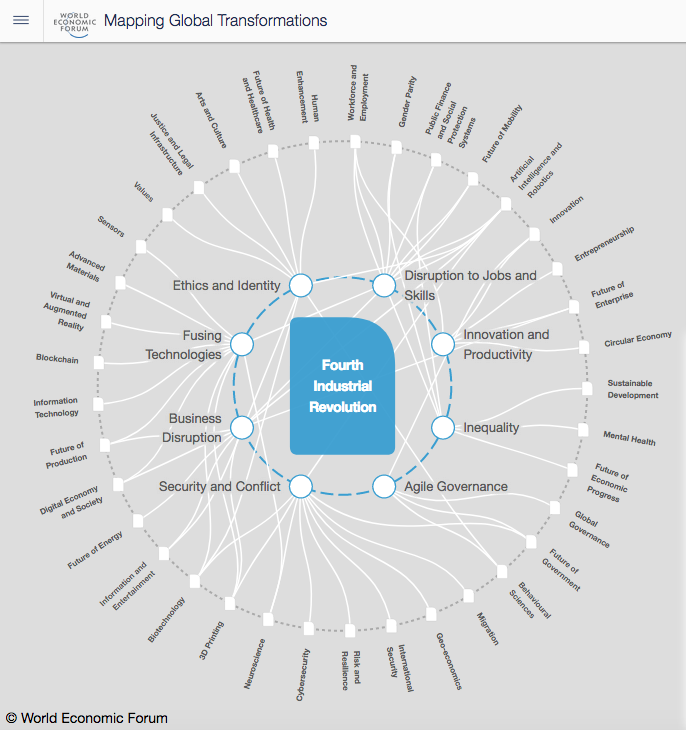
[[](https://www.weforum.org/agenda/2018/02/meet-the-new-renewable-superpowers-nations-that-boss-the-materials-used-for-wind-and-solar)](https://www.weforum.org/agenda/2018/02/meet-the-new-renewable-superpowers-nations-that-boss-the-materials-used-for-wind-and-solar)

**[These renewable superpowers control the future of energy](https://www.weforum.org/agenda/2018/02/meet-the-new-renewable-superpowers-nations-that-boss-the-materials-used-for-wind-and-solar)**

[Andrew Barron · The Conversation 20 Feb 2018](https://www.weforum.org/agenda/2018/02/meet-the-new-renewable-superpowers-nations-that-boss-the-materials-used-for-wind-and-solar)

Explore context

Artificial Intelligence and Robotics

****

[Explore the latest strategic trends, research and analysis](https://toplink.weforum.org/knowledge/insight/a1Gb0000000pTDREA2/explore/summary" \t "_blank)

Stories about killer robots, machine-augmented heroes, laser weapons and battles in space - outer or cyber - have always been good for filling cinema seats, but now they have started to liven up sober academic journals and government white papers.

However, war is about much more than combat or how we fight. Is the sensationalism of high-tech weaponry blinding us to technology’s impact on the broader social, political and cultural context that determines why, where and when war happens, what makes it more or less likely, and who wins?

Consider artificial intelligence (AI). The potential for developing lethal autonomous weapons systems grabs headlines (“killer robots!”), but the greatest impact of AI on conflict may be socially mediated. Algorithmically-driven social media connections funnel individuals into trans-national but culturally enclosed echo-chambers, radicalising their world-view.

As robots relieve humans of their jobs, some societies will prove better prepared than others in their use of education and infrastructures for transitioning workers into new, socially sustainable and economically productive ways to make a living. Less prepared nations could see increasingly stark inequality, with economically-excluded young people undermining social stability, losing faith with technocratic governance, and spurring the rise of leaders who aim popular anger at an external enemy.

Looking beyond individual technologies allows us to focus on the broader and deeper dimensions of the transformation coming our way. Professor Klaus Schwab, chairman and founder of the World Economic Forum, argues that the collapse of barriers between digital and physical, and between synthetic and organic, constitutes a [Fourth Industrial Revolution](https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab/), promising a level of change comparable to that brought about by steam power, electricity and computing.

Something that makes this revolution fundamentally different is how it challenges ideas about what it means to be human. For instance, neuroscience is teaching us more about our own fallibility, and also just how ‘hackable’ humans are. As science continues to uncover difficult truths about how we really operate, we will have to confront basic assumptions about the nature of human beings. Whether this deep transformation will reinforce or undermine a shared sense of human dignity, and what effects it will have on our relationship with organized violence, remain open to question.

The experience of past industrial revolutions can help us begin to search for answers about how this will transform the wider context of international security. In the first industrial revolution, deposits of coal and iron ore were one factor determining the “winners” in terms of economic and geopolitical power.

Today, new modes and artefacts of industrial production will also change demand patterns, empowering countries controlling supply and transit, and disempowering others. Progress in energy production and storage efficiency, for instance, is likely to have profound consequences for the petro economies and the security challenges of their regions. Although the set of natural resources critical to strategic industries will change, their use as a geo-economic tool will probably be repeated.

For instance, this is widely thought to have happened when, in the midst of a maritime dispute with Japan in 2010, China [restricted](http://www.nytimes.com/2010/09/23/business/global/23rare.html?_r=2) export of “rare earths” that are critical for computing, sensors, permanent magnets and energy storage. With ever more commercial and military value embedded in the technology sector, such key materials will be deemed “critical” or “strategic” in terms of national security, and be subject to political as well as market forces.

The 19th Century Industrial Revolution showed how technological asymmetry can translate into geopolitical inequality – in the words of Hilaire Belloc’s poem ‘The modern traveller’, spoken by a European about Africa: “*Whatever happens, we have got the Maxim Gun, and they have not*”. (The Maxim Gun was the first recoil-operated machine gun).

What will be the Maxim Gun of our time? Who will have it, and who will not? In the 20th Century, the “haves and have-nots” of the nuclear weapons club membership became the major determinant of the post-war global order, and – as seen in the cases of Iran and North Korea today - this continues to be relevant. Stealth technology and precision guided missiles used to impose a “new world order” in the early 1990s showed how the gap in military capability separated the United States from others, sustaining its leadership of a “unipolar” order.

According to the current US deputy secretary of defence Robert Work, [“There’s no question that US military technological superiority is beginning to erode”.](https://www.ft.com/content/849666f6-cbf2-11e5-a8ef-ea66e967dd44)

History can only tell us only so much. There is a need for fresh thinking about the implications of the Fourth Industrial Revolution for international security.



**Strategic de-stabilisation**



1. **Waging war may seem “easier”.** If increased reliance on machines for remote killing makes combat more abstract from our everyday experience, could that make it more tolerable for our societies, and therefore make war more likely? Those who operate lethal systems are ever more distant from the battlefield and insulated from physical danger, but this sense of advantage may prove illusory. Those on the receiving end of technological asymmetries have a stronger incentive to find other ways to strike back: when you cannot compete on a traditional battlefield, you look to where your adversary is vulnerable, such as through opportunistic attacks on civilians.



2. **Speed kills.** [“The speed at which machines can make decisions in the far future is likely to challenge our ability to cope, demanding a new relationship between man and machine.”](http://www.defenseone.com/threats/2016/10/future-army/132105/) This was the assessment of US Major General William Hix at a conference on the future of the Army in October 2016. The speed of technological innovation also makes it hard to keep abreast of new military capabilities, easier to be misled on the actual balance of power, and to fall victim to a strategic miscalculation. The fact that some capabilities are deliberately hidden just makes it harder. Because offensive cyber capability relies so much on exploiting one-off vulnerabilities, it is difficult to simultaneously demonstrate and maintain a capability. Once a particular vulnerability has been exploited, the victim is alerted and will take steps to fix it. General Hix again: ["A conventional conflict in the near future will be extremely lethal and fast, And we will not own the stopwatch."](http://www.defenseone.com/threats/2016/10/future-army/132105/)



3. **Fear and uncertainty increase risk.** The expectation that asymmetries could change quickly – as may be the case with new strategic capabilities in areas like artificial intelligence, space, deep sea and cyber – could incentivise risk-taking and aggressive behaviour. If you are confident that you have a lead in a strategically-significant but highly dynamic field of technology, but you are not confident that the lead will last, you might be more tempted to use it before a rival catches up. Enhanced capacity to operate at speed puts security actors into a constant state of high alert, incentivises investment in resilience, and forces us to live with uncertainty. Under these conditions, war by mistake – either through over-confidence in your ability to win, or because of exaggerated threat perception – becomes more likely.



4. **Deterrence and pre-emption**. When new capabilities cause a shift in the balance between offensive and defensive advantage – or even the perception of such a shift -, it could increase the incentives for aggression. For example, one of the pillars of nuclear deterrence is the “second strike” capability, which puts the following thought into the mind of an actor contemplating a nuclear attack: “even if I destroy my opponent’s country totally, their submarines will still be around to take revenge”. But suppose swarms of undersea drones were able to track and neutralize the submarines that launch nuclear missiles? Long-range aerial drones can already navigate freely across the oceans, and will be able to fly under the radar deep into enemy territory. Such capabilities make it possible in theory for an actor to escape the fear of second-strike retaliation, and feel safer in launching a pre-emptive strike against aircraft in their hangars, ships in port, and critical infrastructure, with practically no chance of early warning. Indeed, cyberattacks on banks, power stations and government institutions have demonstrated that it is no longer necessary to fly bombers around the world to reach a distant enemy’s critical infrastructure without early warning. The idea of striking a `knockout blow` may come to seem feasible once more.



5. **The new arms race is harder to control**. One of the mechanisms for strategic stability is arms control agreements, which have served to limit the use of nuclear, biological and chemical weapons. When it comes to the multiple combinations of technology we see as a hallmark of the Fourth Industrial Revolution, one of the obstacles to international agreement is caused by uncertainty about how strategic benefits will be distributed. For instance, the international community is currently debating both the ethics and practicality of a ban on the development of lethal autonomous weapons systems. One of the factors holding this debate back from a conclusion is a lack of consensus among experts about whether such systems would give an advantage to the defender or the attacker, and hence be more likely to deter or incentivize the escalation of conflict. Where you stand on the issue may depend on whether you see yourself as a master of the technology, or a victim. Another obstacle to imposing control is the wider cast of players -

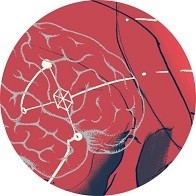


6. **A wider cast of players.** As cutting-edge technology becomes cheaper, it spreads to a wider range of actors. Consider the development of nuclear bombs – the last breakthrough in weapons technology that re-wrote the rules of international security. Although the potential for a fission bomb was understood in terms of theoretical physics, putting it into practice involved thousands of scientists and billions of dollars – resources on a scale only a few nations could muster. Over 70 years later, the club of nuclear weapons states remains exclusively small, and no non-state actor has succeeded in acquiring nuclear capability.

In contrast, there are more than [70 nations](http://spacenews.com/sponsored/growing-imperative/) operating earth-orbiting satellites today. Nano-satellites are launched by Universities and Corporations. A growing list of companies can launch and recover payloads on demand, meaning even small states can buy top-notch equipment “off the shelf”. As [Christopher Zember](http://warontherocks.com/2016/04/the-democratization-of-science-ushers-in-a-new-world-order/) put it, “Once the pinnacle of national achievement, space has become a trophy to be traded between two business owners”. These days, even a committed enthusiast can now feasibly do genetic engineering in their basement. Other examples of dual-purpose technologies include [encryption, surveillance, drones, AI and genomics](https://www.weforum.org/agenda/2016/06/should-we-embrace-the-rise-of-killer-robots/). With commercial availability, proliferation of these technologies becomes wider and faster, creating more peer competitors on the state level and among non-state actors, and making it harder to broker agreements to stop them falling into the wrong hands.



7. **The grey zone**. The democratisation of weaponisable technology empowers non-state actors and individuals to create havoc on a massive scale. It also threatens stability by offering states more options in the form of “hybrid” warfare and the use of proxies to create plausible deniability and strategic ambiguity. When it is technically difficult to attribute an attack – already true with cyber, and becoming an issue with autonomous drones – conflicts can become more prone to escalation and unintended consequences.



8. **Pushing the moral boundaries**. Institutions governing legal and moral restraints on the conduct of war or controlling proliferation date from an era when massively destructive technology was reserved to a small, distinct set of actors – mostly states or people acting under state sponsorship. The function of state-centric institutions is impaired by the fact that states’ militaries are no longer necessarily at the cutting edge of technology: most of the talent driving research and development in today’s transformative dual-use technologies is privately employed, in part because the private sector simply has access to more money. For example, the private sector has invested more in [AI research and development](https://www.youtube.com/watch?v=GYQrNfSmQ0M) in five years than governments have since AI research first started. Diminishing state control of talent is epitomised by Uber`s recruitment of a team of robotics researchers from Carnegie Mellon University in 2015, which decimated the [research effort](http://www.wsj.com/articles/is-uber-a-friend-or-foe-of-carnegie-mellon-in-robotics-1433084582) they had had been working on for the United States department of Defence.

The fact that the trajectory of research – and much of the infrastructure critical to security – are in private hands need not be a problem if state actors were able to exercise oversight through traditional means such as norms development, regulation and law-making. However, the pace and intensity of innovation, and difficulty of predicting what new capabilities will be unleashed as new technologies intersect, makes it difficult for states to keep up. State-centric institutions for maintaining international security have failed to develop a systematic approach to address the possible long-term security implications of advances in areas as diverse as nanotechnology, synthetic biology, big data and machine learning. Nor have industry-led measures yet filled the gap.

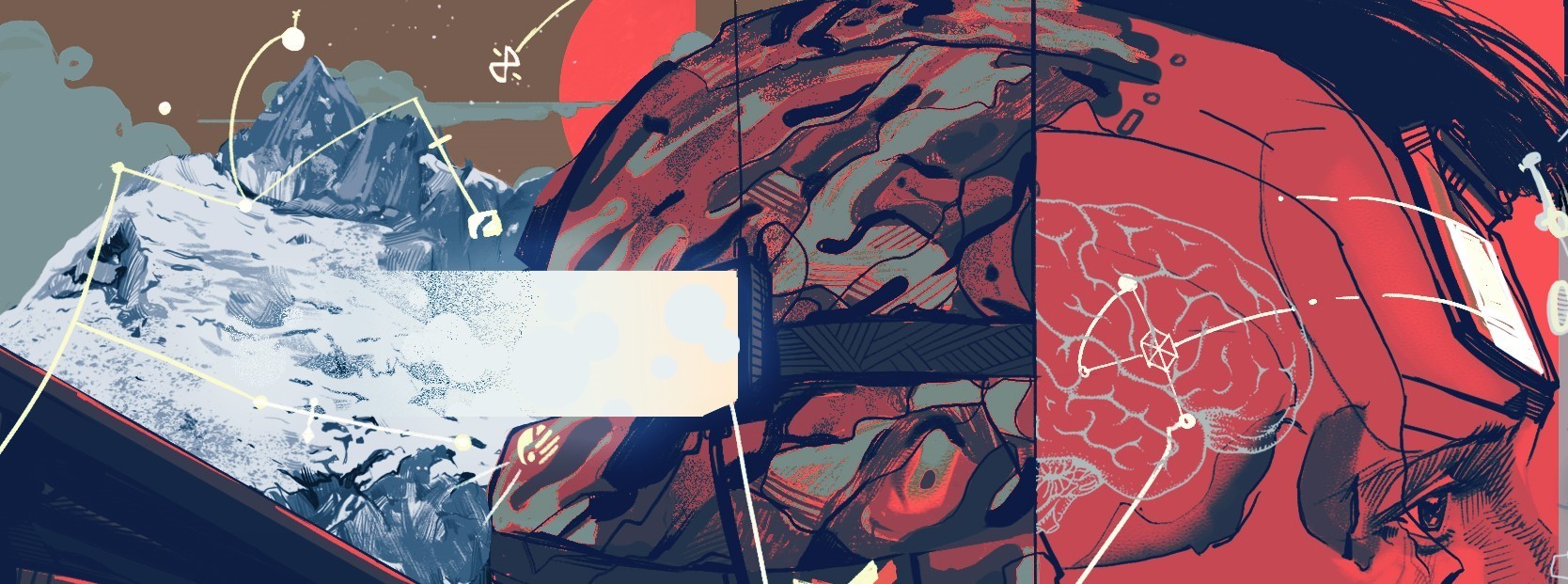


9. **Expanding domains of conflict.** Domains of potential conflict such as outer space, the deep oceans, and the Arctic – all perceived as gateways to economic and strategic advantage – are expanding via new technologies and materials that can overcome inhospitable conditions. Like cyberspace, these are less well-governed than the familiar domains of land, sea and air: their lack of natural borders can make them difficult to reconcile with existing international legal frameworks, and technological development is both rapid and private sector-driven, which makes it hard for governance institutions to keep up.

Those who secure “first mover” advantage may also seek to defend it against the establishment of regulation and governance in the common interest. Access to the technology needed to reach and exploit space, for example, allows belligerents to compromise the effectiveness of defensive measures that rely on satellites for communications, navigation, command and control technology. Even a very limited strike on a satellite would likely cause space debris, damaging systems used by the wider community. Despite a 1967 United Nations treaty calling for the peaceful use of Space, the [United States Deputy Secretary of the Air Force](http://www.cbsnews.com/news/rare-look-at-space-command-satellite-defense-60-minutes/) recently warned that “there is not an agreed upon code of conduct” for space operations.



10. **What is physically possible becomes likely**. History suggests that any technology – even one that gives moral pause - will eventually be developed in order to be used as a weapon. As the political theorist [Carl Schmitt](https://en.wikipedia.org/wiki/State_of_exception) explained, political conflict is the “realm of exception” in all sorts of ways that make the morally unthinkable not only possible, but more likely. Professor [Ole Wæver](https://en.wikipedia.org/wiki/Ole_W%C3%A6ver) and the Copenhagen School of international relations developed the concept of “[securitisation](http://s3.amazonaws.com/s3.libraryofsocialscience.com/pdf/Lipschutz--On_Security-3--Waever-Securitization.pdf)” to describe how a security actor invokes the principle of necessity as a way of getting around legal or moral restraints. Policy-makers can argue that because non-state actors, terrorist and criminal groups can access new technology, they are obliged to pursue weaponization, in order to prepare an adequate defence. Public disquiet can also be bypassed by conducting research in secret; we now know from de-classified accounts of Cold War studies that soldiers were used as guinea pigs to research the effects of new weapons, and military experiments may well be underway today in areas such as [human enhancement](https://www.foresight.org/policy/brief2.html). The tendency for the logic of conflict to drive the development of technology beyond what is considered acceptable by society under normal conditions is one more reason to pay closer attention to trends in this field.



**Institutional shifts**

**International Security** is destabilised at the institutional level by the way the 4th Industrial Revolution is empowering the individual through technology, and the way that [blurs the lines](https://www.weforum.org/agenda/2016/02/is-technology-blurring-the-lines-between-war-and-peace/) between war and peace, military and civilian, domestic and foreign, public and private, and physical and digital. The [democratisation of destruction](http://foreignpolicy.com/2011/08/15/get-ready-for-the-democratization-of-destruction/) has been mentioned above, but non-state groups’ leveraging of global social media - whether to gain support, undermine the morale of opponents, sow confusion, or provoke a response that will create an advantage - has increased the strategic importance of shaping perceptions and narratives about international security. ISIS’s use of online videos provide an extreme example of a non-state actor using social media to drive recruitment, while state security services in select countries employ online “trolls” on a large scale. Consider the implications for democratic control over armed force when technologies like big data analytics, machine learning, behavioural science and chatbots are fully enlisted in the battle over perceptions and control of the narrative.

The [hacking attack suffered by Sony Pictures Entertainment in 2014](https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation), allegedly motivated by North Korea’s political grievance, highlights these blurring lines – and the resulting difficulty of deciding who should be responsible for security in this new reality. If someone were so offended by a movie that they burned down the studio’s warehouse, one would expect the police to step in. But is it ultimately the responsibility of the state or of corporations to prevent or deter the kind of attack experienced by Sony Pictures? What is the appropriate response? When does an attack on a private company constitute an act of war? As an increasing proportion of what we value gets uploaded onto a global infrastructure of information and communications technology, do we expect it to be protected by service providers like Apple, or by our state’s security agencies?

Little by little, the responsibility for defending citizens is effectively shifting away from the state and towards the private sector. It is, for example, your bank’s security chief who bears responsibility for protecting your money from international cyber theft, whether it comes from straightforward criminal groups or those acting under the [sponsorship of sovereign states](http://www.npr.org/sections/thetwo-way/2016/05/27/479760450/north-korea-linked-to-81-million-bangladesh-bank-heist). A [report](http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf) by Internet security company McAfee and the think-tank CSIS estimated the likely annual cost to the global economy from cybercrime at more than $400 billion – roughly equivalent to the combined defence spending of the European Union, or the Asia region.

According to 17th century political theorist Thomas Hobbes, the citizen agrees to give up some freedom and render loyalty in exchange for protection and to escape the “natural condition” of life, which was otherwise “solitary, poor, nasty, brutish, and short”. In return, the state expects respect for its laws. But if citizens lose confidence in the state’s capacity to guarantee their security, be it through military protection or domestic justice and policing or social safety nets, they may also feel less of an obligation to be loyal to the state in return. In effect, the unravelling of the Hobbesian ”social contract”. This can undermine mechanisms for global governance, which consist of inter-state institutions that rely on state power for their effectiveness.

Could the relative loss of state power fatally undermine the system of international security? Several well-known tech entrepreneurs have talked in ways that suggest they see national governments not as a leader in norms development, but as an unnecessary inconvenience. Genetics innovator Balaji Srinivasan has envisioned [“Silicon Valley`s ultimate exit”](http://genius.com/Balaji-srinivasan-silicon-valleys-ultimate-exit-annotated) from the USA. Paypal co-founder Peter Thiel has floated the idea of establishing a sea colony to literally offshore himself from government regulation. Elon Musk has talked about [colonising Mars](https://www.wired.com/2016/09/elon-musk-colonize-mars/). There is serious interest in [businesses formulating their own foreign policy](https://hbr.org/2016/09/why-your-company-needs-a-foreign-policy). These are interesting ideas, but until there is a credible rival the state for the role of main international security actor to meet the challenges of the Fourth Industrial Revolution, the character of state action on security will need to adapt to the new environment, re-position itself to accommodate other actors, and renegotiate relations across a widespread network of partnerships.



**What is to be done?**

As attitudes adapt to the new distribution of security responsibility between individuals, companies and institutions of governance, there is a need for a new approach to international security. There is plenty of room for debate about how that approach should look, but the baseline can be drawn through three points: it will need to be able to think long-term, adapt rapidly to the implications of technological advances, and work in a spirit of partnership with a wide range of stakeholders.

Institutional barriers between civilian and military spheres are being torn down. Outreach to Silicon Valley is a feature of current US Defence policy, for example, as are invitations to hackers to help the Department of Defence to maintain its advantage in the digital domain. The “third offset strategy” promoted by US Defence Secretary Ashton Carter is based on a recognition that private sector innovation has outstripped that of military institutions in the post-Cold War era, and a more open relationship with business as well as with academic and science institutions could prove vital to maintaining the dominance of US military capabilities.

Such is the speed, complexity and ubiquity of innovation today, we need a regulation process that looks ahead to how emerging technologies could conceivably be weaponized, without holding back the development of those technologies for beneficial ends. “Hard governance” of laws and regulations remain necessary, but we will also need to make more use of faster-moving “soft governance” mechanisms such as laboratory standards, testing and certification regimes, insurance policies and mechanisms like those set up by academics to make potentially dangerous research subject to approval and oversight. This will need to proactively anticipate and adapt to not only technological changes, but also macro-cultural ones, which are a lot harder to predict.

States and other security actors need to start exploring with each other some of the concepts and modes of operation that would make such a networked approach sustainable, legitimate and fit for the ultimate purpose of maintaining stability and promoting peaceful coexistence in the emerging international security landscape.

Instead of meeting each other in court, as the [FBI met the Apple](http://money.cnn.com/2016/03/21/technology/apple-fbi-tuesday/) Corporation to settle their dispute about encryption, security providers could meet across a table, under new forms of public oversight and agile governance, as partners in a common endeavour. Instead of struggling along in denial, or wasting energy trying to fight the inevitable, stakeholders who have been working in parallel siloes can learn to collaborate for a safer world. What cast of actors populate this wider security ecosystem? What are shared priorities in terms of risks? What are some of the potential models for peer to peer security? How can the 4th Industrial Revolution be used to give citizens a stronger sense of control over choices of governance, or to deny space to criminal organizations and corrupt practices? Can [smart contracts using block chain technology](http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24) be applied to build confidence in financial transactions and peace agreements? Can defensive alliances be expanded to include or even consist entirely of non-state actors? Should international law extend the right to use proportionate force in self-defence in cyber conflict to commercial actors? What aspects of these challenges are a matter for legal instruments and regulation, and what aspects will require a new approach?

The future of national security may lie in models of self-defence that are decentralised and networked. As Jean-Marie Guéhenno, CEO of the International Crisis Group, wrote: [“distribution of security measures among a multiplicity of actors – neighbourhoods, cities, private stakeholders – will make society more resilient. And over time, smaller but well-connected communities may be more effective at preventing and identifying terrorist threats among their members](http://blog.crisisgroup.org/worldwide/2016/02/19/the-cybersecurity-paradox/).” Several of the critical ingredients of such a de-centralized model are becoming available: more security responsibility is being taken up by city mayors and even civil society groups like the global hacktivist collective “Anonymous”, who declared war on the self-styled Islamic State. So far, however, this has been a haphazard phenomenon and its impact is diminished by a lack of coordination.

The answers that may emerge to these questions are unpredictable – but what is clear is the need to have a conversation that reaches across generations and across disciplines. This conversation has to be global. International security is threatened by a loss of trust, in particular between those who drew power from the last industrial revolution and those whose power is rising within a fluid and complex environment. The conversation needs to foster mutual understanding, dispel unjustified fears, and revive public confidence in new forms of responsive leadership that manifestly serve the common good.

*This article is based on a World Economic Forum project on the relationship between the Fourth Industrial Revolution and International Security, drawing on conversations at a number of World Economic Forum events in 2015 and 2016. The authors would like to thank to Klaus Schwab, Jim Snabe, Isabel de Sola, Andrew Fursman, Jean Marie Guéhenno, Natalie Hatour, Yoichi Funabashi, Ramya Krishnaswamy, Juergen Keitel, Paul Scharre, Nell Watson, Andrew Wright and Christopher Zember (and colleagues at NDU) for invaluable comments and input.*

Share

Written by

[Anja Kaspersen](https://www.weforum.org/agenda/authors/anja-kaspersen), Former Head of Geopolitics and International Security, World Economic Forum

[Espen Barth Eide](https://www.weforum.org/agenda/authors/espen-barth-eide), Member of Parliament, Parliament of Norway

[Philip Shetler-Jones](https://www.weforum.org/agenda/authors/philip-shetler-jones), Programme Lead, International Security, World Economic Forum

The views expressed in this article are those of the author alone and not the World Economic Forum.

Haut du formulaire



Bas du formulaire