PARTNERSHIP FOR PEACE CONSORTIUM
BACKGROUND PAPER

Technology Innovation and Its Impact: Policy Considerations for International Security

PfPC Emerging Security Challenges Working Group Background Paper No. 2 | July 18, 2014 | www.pfpconsortium.com

Do-it-yourself drones and guns are already a reality. But innovation is apt to make existing designs even more powerful – and dangerous.

EXECUTIVE SUMMARY

"Emerging Security Challenges" is an all-encompassing term used to describe a set of non-traditional threats and risks that increasingly impact our security policy agendas. Many of these are linked to new or evolving technologies – requiring careful consideration of their potential implications.

Addressing such issues requires knowing and understanding new technologies and – in particular – the way in which they impact security policy making. This is easier said than done, as there is constant and rapid innovation which policy makers have to be aware and keep track of. Developments in remote warfare, 3D-printing, nanotechnology, big data, and the "Internet of things" are all dependent on advances in information technology that herald potentially disruptive political and societal change.

Setting the Context

This paper addresses policy issues arising out of the rapid development of technology innovation and their potential and real impact on TODAY's policy making. This process can be called "disruptive innovation" and will continue, presumably at increasing speed.

These developments create two related, not compatible types of problems:

1) *Speed* – The speed of technological innovation becomes an increasingly critical element of policy making, as it becomes progressively more complex for individual actors to keep track of rapid developments. Moreover, increased speed of computer technology development leads to increased quantities of information which need to be handled. As a result, policy makers run the risk of being submerged and overtaken by developments at every turn.

2) *Contradiction* – While policy makers have an increasingly difficult time grasping the implications of new and rapid innovations, especially those taking place in a space without physical barriers (in cyber space, for example), they may need, on the other hand, to create specific processes to allow for an open, deliberate and democratic, this means control-lable, decision-making process; for this process, time for reflection and discussion is of essence. Decision makers are squeezed between the increasing speed of technological innovation and the increasing need for time to understand, manage, and explain what they are doing in an increasingly complex communication environment.

Emerging Challenges are Real

Remote Warfare

Technological innovation enables warfare over long distances, drastically reducing the need to place military personnel in harm's way. This is of particular importance, as military commanders always seek to lower soldiers' fatality and injury risk. This sentiment is shared by political decision-makers who realize that public opinion can shift rapidly in case of casualties and fatalities. Many remote warfighting tools already exist, and others are being developed: drones, remote AI (Artificial Intelligence)-driven snipers, air-delivered IEDs (Improvised Explosive Device), quadcopters, UGVs (unmanned ground vehicles), robotic aircraft, DIY (Do-It-Yourself) tracking devices, precision mortars and rockets, and many more.

To a certain degree, all of these objects can be built or purchased on the open market. Some are simply do-it-yourself projects. To function effectively, some depend on communication networks, most often existing civilian networks. This is a situation in which a military operation may become vulnerable, as communications can be jammed or manipulated, affecting spectrum dominance.

With respect to autonomous weapons systems, the U.S. Department of Defense has adopted a policy that underlines the need to design such weapons so that human operators can override pre-programmed targets. However, human operators most often don't have the time to choose between a multitude of pre-programmed targets, but will do what the systems recommends. The challenge here is not only to reduce increasing vulnerability to a maximum, but, even more important, to secure human control over every phase of war fighting.

3D-Printing

At the same time, new technology allows for the manufacturing of goods through addition of multiple layers of plastic, metal, ceramics or other materials. Thus, potential consumers can create for themselves their desired product at relatively low cost, including weapons and other products necessary or useful for war fighting. Currently, there are over 50 materials which can be used in 3D-printers. Considerable questions concerning this way of production still remain to be solved, including issues surrounding design and intellectual property, quality control, and liability. The challenge for security policy officials is that it may become easier in the future to copy critical technologies and to lose control over production and proliferation of certain types of weapon systems, particularly as printers become more precise and new materials become available. DIY drones and guns are already a reality, but innovation in 3D-printing is apt to make existing designs even more powerful. The promise of reduced energy and material waste drives much 3D-printing development, but questions remain there too.

Nanotechnology

Over the past decade, computing technology has also enabled major leaps in the science and the development of nano-sized devices. Silicon nanowires of 2 nm (nanometers), transistors as small as 3 nm, and many more devices at under 10 nm can now be produced and used in communication and weapon systems. Research is still in a pre-competitive stage and wide open, but U.S. industries have started monetizing it. Strategic challenges arise out of the fact that, besides the U.S., only Japan and South Korea work on this issue in a substantial way – very little is being done in Europe.

Will this create or deepen dependencies, which our policy makers are then subject to? Another challenge related to advances in nanotechnology is the vast amount of energy needed to supply power for nano electronics. Around 500,000 data centres in the world consume substantial amounts of power, each one averaging the energy consumption of a small city. Some even say that about half of this energy is wasted – compounding the scope of the challenge. Today, energy expenditures for data centres cost more than the data centres themselves. Energy efficiency thus is the next technology driver. But what and who drives energy efficiency?

Internet of Things

The Internet of Things (IoT) is about communication between machines, commonly referred to as Machine-to-Machine (M2M) communication. Analysts predict that because of our ability to potentially connect billions of machines together through low cost sensors, society will materially gain through increased energy efficiencies and devices which will take on more of the burden. At present, the IoT has many proponents in industry, notably Cisco and IBM, among other powerhouses. While the IoT may be the beginning of a new industrial revolution, little is being written about the potential security risks that come with connecting all the world's devices. If the rise of the Internet has taught us anything about risks associated with increased connectivity, policy makers should be especially careful to regulate the IoT's security protocols. It is one thing to have email go down, or your bank account hacked, and yet another order of magnitude when it is physical devices that fail in ways that cannot be easily remedied and that bear unforeseen consequences. The IoT is likely to breed a new brand of cyber risk.

Industry

Finally, communication technology as well as ICT protection systems are developed and marketed by private industry. About 90% of all security relevant communication networks are owned and operated by the private sector. Given this reality, it is therefore essential that security policy makers and industry cooperate closely on security matters. Hardware and software providers have every interest in protecting their customers' interests, but they also have a vested interest in making money. Policy makers have every interest in acquiring equipment with the highest possible security standards. After the first revelations by Edward Snowden on NSA/GCHQ activities for example, there has been a major push to acquire cyber warfare capabilities, including offensive capabilities, as Kaspersky Labs noted. We are, therefore, confronted with another challenge; while we depend more heavily than ever before on cooperation with industry on very sensitive state matters, understanding and handling potential conflicts of interest between the private and the public actors becomes more critical.

Policy Considerations

To address these issues, policy makers would do well to reflect upon the following considerations.

1 **Establish a regular and trusted relationship between technological innovators and policy makers**. **Raise awareness of the technological innovators' security responsibility.** Decision-makers or shapers are often overwhelmed or unaware of technological innovation that takes place in their field of activity. Or, for fear of being considered unaware, they do not dare ask questions concerning new technical developments. Yet, in the field of security policy, the technical and the political spheres need to cooperate closer and on a regular basis, not just in case of an urgent need. As technical performance continues to grow exponentially, those who shape and make policy need to fully understand the way in which the instruments for their activities impact security. They need to know, understand what is available and anticipate what may be developed. It is increasingly clear that policy makers must grapple with reality and not leave all technical matters in the hands of science and industry.

2. **Agree on an international regime or the applicability of existing international law to deal with autonomous weapon systems.** Human actors must maintain control over the use of weapon systems at all times. As technology advances and automated warfare with or without minimal human interference becomes a real possibility, it is important to seek an international agreement to either ban, limit the use, or agree on the use of autonomous weapons systems – similar to international agreements on bans on certain types of weapons or comparable to arms control regimes. Human control on action, in particular on action with potentially fatal consequences, has to be maintained under all circumstances.

3. **Follow closely developments in the technology of 3D printing and its impact on proliferation**. Although still in an early experimental phase, 3D printing has great potential for the production (and proliferation) of home-made, sophisticated weaponry. The state, as guarantor of public interest and security, should ensure that production of and trading with weapons remains under close control.

4. **Increase efforts to reduce – and not increase – dependency on energy as data computing extends**. In supplying the necessary power for our increasingly technology-driven society, including nanoelectronics and the storage of vast quantities of information, a lot of energy is being wasted. This increases the dependency and vulnerability of our communication networks and critical infrastructure. Efforts should be undertaken to mitigate all use of energy to safeguard the environment and enhance sustainability.

5. **Establish reliable formats of cooperation between the public and the private sector.** Increasing dependency of security policy makers on communication networks translates into increased

dependency on private business, which invents, develops, produces, and most often owns and runs these networks. The private sector does not work in the public good; it has a profit maximizing objective. As a result, it encourages government de- regulation, as these sectors are very dynamic. Government, on the other hand, works towards the common good and has to secure the best possible protection and be able to provide the necessary in-house expertise to match industry. A new way of cooperation has to be developed in this era of fundamental change.

This background paper was prepared by Sean Costigan, Dr. Gustav Lindstrom and Dr. Detlef Puhl based on recent meetings of the PfP Consortium's Emerging Security Challenges Working Group.

CONTACT INFORMATION

For more information, please contact:

PfPC Emerging Security Challenges Working Group Co-Chairs

Dr. Gustav Lindstrom, Head, Emerging Security Challenges Programme
Geneva Center for Security Policy
G.Lindstrom@gcsp.ch

Dr. Detlef Puhl, Senior Advisor, Emerging Security Challenges Division, NATO International Staff
Puhl.Detlef@hq.nato.int

PfPC Emerging Security Challenges Working Group Senior Adviser

Mr. Sean Costigan, The New School
sean_costigan@post.harvard.edu

OR

International Program Manager, The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

Mr Frederic Labarre,
Frederic.Labarre@marshallcenter.org
+ 49 8821 750 2359

OR

The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Operations Staff:
pfpconsortium@marshallcenter.org
www.pfpconsortium.com