GCSP
Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

Impartial, Inclusive, Influential

GCSP Policy Paper 2013/5

29 July 2013

Emerging Security Challenges: Framing the Policy Context

by Graeme P. Herd, Detlef Puhl and Sean Costigan

Key Points

- *Security challenges are 'emergent' or 'emerging' when the wider community of security experts begin to discuss and debate a given issue as a prelude to developing, resourcing and then implementing appropriate policy responses.*
- *Some security challenges are "ab ovo" – they emerge onto the policy landscape at incredible speed, complete and entire, rather than slowly over a long gestation period.*
- *For some institutions, the 'real' emerging challenge is defined as much by institutional and cultural change needed to enable more efficient, effective and legitimate policy response as it is by the inherent complexity of the challenges themselves.*
- *Highest priority challenges (e.g. climatological, nuclear, biological, health and agriculture-related) are those that threaten the survival of people and institutions. Second order priority challenges undermine essential ways of life and the fabric of state-society relations, the nature of democratic governance and the integrity of the 'social contract'.*

What is an Emerging Security Challenge?

'Emerging Security Challenges' is a contested notion, commonly used to distinguish a more recent set of threats from what is considered a mainstream or 'traditional' security agenda. Often and for the few institutions that address such issues, this term becomes a default catch-all for all 'non-traditional' threats, rather than a category defined by the essential nature of the challenges in question.

Our understanding of the scale, scope and significance of emerging security challenges and which policy responses are acceptable, affordable and appropriate are conditioned by two subjective factors: first, who 'we' are (individual, society, state, region, planet); and second, what 'we' consider to be 'emerging' and what is already 'emerged'. In our working definition, security threats and challenges are actions or events that put at risk the material or identity basis upon which individuals, societies, states and perhaps even the planet have come to expect or rely.

From that vantage point, we can posit at least three characteristics that provide positive criteria ('what it is' rather than 'what it is not') to better capture the notion of emerging security challenges. The first concerns the meaning and status of 'emerging' as opposed to new or traditional. The second concerns the genealogy or pathway by which challenges move from obscurity to become apparent and prominent. The third concerns the nature of the challenges posed by certain types of threats - here the focus in terms of emergence is on the nascent characteristics of policy responses.

'Many are called, few are chosen'

Security challenges can be considered as 'emergent' or 'emerging' when the wider community of security experts begin to discuss and debate a given issue as a prelude to developing, resourcing and then implementing appropriate policy responses. Many potential issues are called security risks and challenges but fewer are more fully and seriously debated as such. For this to occur, authoritative 'gatekeepers' within the community of security experts need to identify and then elevate particular issues from generalised informal discussion to the policy agendas worthy of governmental or institutional policy consideration. How do we know this when we see it? A rough metric might be: if a security challenge is published in an issue of

Foreign Affairs or another authoritative and respected publication, or if a securitizing actor (for example, a government or UN agency, a respected NGO, public intellectual or multinational corporation) produces a major study of the issue, then it has clearly emerged, having reached a level of public awareness that likely makes it embedded within the wider analytical community's discourse and agenda.

Following the logic of 'elevated authoritative awareness', issues such as the proliferation of chemical, nuclear, biological, and radiological weapons are all security challenges. They cannot be considered emerging security challenges since in each case we have moved beyond discussion and debate of policy responses to agreed policy implementation with a range of relevant actors – from states with regards to non-proliferation to international organisation- taking a lead. Admittedly, the effectiveness, efficiency and legitimacy of elaborated policy responses and their implementation can be questioned and policy response adaptation is a continuous process, but nonetheless discussion leading to action has occurred.

Recent scientific breakthroughs across a range of fields have a clear potential for security impacts, most notably in nanotechnology, biology and genetic research, robotic and cognitive sciences, information and communication science, materials science, chemistry and physics, neurosciences and medical sciences. The inter-enabling aspect of these technologies – 'the changing, new, or novel application of knowledge, both in terms of development and use' - suggests that latent threats and challenges can, through convergence, become potential and then real.

What does the transition from emerging security challenge to other type of challenge resemble? First, authoritative reports are written on many issues that then receive widespread attention without moving beyond discussion to policy responses, let alone to policy implementation. Second, some strategic threats – regional crises and fragile states, terrorism and political extremism, for example – are constantly mutating and continuously manifest themselves in different guises and locales, requiring the formation of new policy approaches and responses to address the new security challenges posed. Considering cyber attacks, for example, the Obama administration has stated they will reserve kinetic response as an option for cyber strikes, but these policies are very immature. Third, other challenges, such as those from climate change and resource scarcity-induced conflicts remain latent though they might still emerge as actual challenges in 20 to 30 years, the challenge can be considered to be emerging right now. Fourth, for some other identified challenges policy responses are extremely premature. Security for space-tourists and colonists would, for example, fall into this category.

'Unbounded' Innovation

Some security challenges are "ab ovo" – they emerge onto the policy landscape very suddenly, complete and entire, rather than slowly over a long gestation period. Often this shift from relative obscurity to front-stage occurs with incredible speed. The science behind the atom bomb was ongoing for years before the creation of the bomb, but might be considered one such example.

Such 'unbounded innovation' highlights the need to consider, understand and anticipate the direct and indirect effects of the application but reduces the time in which such reflection can take place. For example, ubiquitous advances and cost reductions in computing, navigation and hobbyist technologies are apt to reduce barriers to remote and other forms of warfare, bringing new and disruptive capabilities into the hands of current or potential adversaries, or completely autonomous, irresponsible groups of people or individuals ('clans and gangs') without any mandate. Consider two cases in point: information technologies can easily create crowds and amplify unrest, yet they are not as useful for controlling crowds; low price navigation in smartphone's is helpful to people and commercial interests, yet these phones have everything needed to acquire and navigate to potential targets.

Many though not all emerging security challenges are hatched as a result of rapid technological developments and these include:

- enhanced and extreme longevity and its associated economic and demographic issues;
- genetic modification and sub-speciation (the ability of humans to self-modify genetically) and the potential backlash against human, plant or environmental modification;
- planetary defence against asteroid and meteor strikes; state responses to climate change, such as geo-engineering, that could result in clashes to prevent modification to the bio-sphere;
- artificial and computer or via computer simulation (in-silico) intelligences;
- designer pathogens;
- sub-national groups and individuals employing Intelligence-Surveillance-Reconnaissance (ISR)-precision strike complexes;
- Do-it-Yourself (DIY) laser enrichment and manufacture of small yield nuclear weapons; and 3D printing of precision detonators or other weaponry.

Some elements on this list are more than decade away, and others may appear tomorrow. This list is indicative and far from being complete but, while still rooted in today's realities, goes far beyond what NATO or governments have labelled as being emerging security challenges.

'Policy response as the emerging security challenge'

For some institutions, the 'real' emerging challenge is defined as much by institutional and cultural change needed to enable more efficient, effective and legitimate policy responses, as it is by the inherent complexity of the challenges themselves. At NATO, for example, an Emerging Security Challenges Division addresses cyber security, counter-terrorism, counter-proliferation and energy security. However, there is little or no consensus

among member states on the substance and scope of the issues to be dealt with by the organization. Energy security, counter-proliferation and counter-terrorism are not 'emerging' or 'new' security challenges *per se*. These particular challenges appear to be classified as 'emerging security challenges' because either necessary policy responses do not fit into pre-existing traditional policy making structures and approaches within the organisation, or appropriate responses span several policy-making and implementing structures. Thus, for NATO the 'real' emerging challenge seems to be whether and how it has to change policy-making and policy response implementation to effectively provide security from changing, though not necessary new, threats.

Throughout the 20th and still new 21st century, governments have systematically underestimated the disruption possible from technology and scientific advances. Despite calls to more deeply analyse emerging threats, many policy-making and military organisations are not built to do such work. Massive information flows lead to overload, creating difficulties for functioning states to coordinate and prioritize action. The norm is for institutions to "wait for change" or, in other instances, to learn lessons from the last war and thus be doomed to be unprepared. Cognitive biases, cultures that are averse to change, and diverging political or other interests may very well prevent us from enabling awareness. While the pace of scientific discovery and technological developments grows exponentially, when it comes to recognizing long term security challenges, human brains may still behave in a linear, sequential mode. As a result, present policy institutions remain ill prepared to address the speed at which emerging and new technologies create vulnerabilities, risks and threats.

As development life cycles shorten dramatically, technologies reach a level of maturity before securitization has taken place. Today, we may be obliged to think of securitisation almost at the point of innovation; and the next wave is almost immediately behind. And yet securitisation comes with risks to innovation and may threaten advancement. The following list of trends shaping the use and abuse of emerging and existing technologies is illustrative of the challenge of understanding and keeping pace with the potential or actual threats they pose and responding to mitigate risk. While not exhaustive, these trends are also characterized by their multiple inter-relationships:

Miniaturisation	Automation
Connectedness	Availability
Affordability	Proliferation
Democratisation	Dependence
Globalisation	Vulnerability
Transdisciplinarity	Digitisation
Pervasiveness	

So What? Strategic Implications

Emerging security challenges place greater stress and tension on the necessary balance between bed-rock principles, norms and values of societies. For example, digital technologies have increased stress on the dynamic between individual and societal freedom of expression and right to privacy versus the obligation and duties of states to protect its citizens. Fundamental questions about the fabric of state-society relations, the nature of democratic governance ('are democracies dysfunctional?') and the integrity of the 'social contract' is raised. Does the 'social contract' need to be defended, preserved or adapted? The implications of emerging security challenges for democratic policy making and international cooperation are clearly centred on determining an appropriate, acceptable and affordable equilibrium between upholding democratic values and structures of cooperation while efficiently and effectively addressing such challenges.

To that end we can ask: are these issues part of current education and so can be expected to inform the intellectual and conceptual formation of our security and defence institutions? Can our political leaders (decision-makers and shapers) address these issues in a responsible and democratic fashion? In many sectors and areas of the world, security challenges are deeply rooted in longstanding cycles of repetitive behaviour. It would be too easy and dangerously costly for our democratic leaders to ignore the emergence of the future, as complex and dangerously unpredictable as it is. Only utmost openness of mind allows us to explore these complexities. And policy-making institutions need to allow for this openness of mind to be expressed and shape the way in which new challenges can be met in a democratic fashion.

For the state, ramifications should be considered at early stages of research and development (R&D). But would early thinking about security concerns derail development? For example, the Internet was developed without security concerns, and is a testament to the ideal of problem-solving and openness; but the developers put a premium on access and sharing over security, unwittingly opening a new door to criminality, espionage and terrorism. How, then, can governments regulate R&D, balancing the need to stimulate R&D while exercising control over research whose outcomes may lead to security challenges? Is the policy to control basic research or is it to control the applications of such research? At what point do states/societies decide to exercise control, and how might this be enacted? Is each case different?

Increasingly we appear to be switching from 'spin off' technologies (from military to civilian use) to 'spin-on' technologies (from civilian to military use). As a result, rogue states, violent or criminal non-state actors and fragile states all can have access to technology. The risk calculus of democratic states is changing. Multiple positive/negative applications beyond traditional

'dual use' functionality and effect also exist in tandem. Indeed, some technologies represent mitigation opportunities for the very challenges and threats they may generate. For example, does the increased pace of technological developments mitigate or exacerbate the tension between aging populations', the food, energy, water nexus and economic well-being? Has this pace advantaged or disadvantaged the role of individuals or small groups' versus nations and alliances in maintaining global stability?

Food, Energy, Water Stress Nexus
Shell, Royal Geographical Society, 2012

Now What? Policy Considerations

At the minimum, responsible democratic leadership has to be aware of developments that could threaten the security of the state, society and individual. Awareness produces the opportunity for action and, potentially, better outcomes. Such awareness generation typically begins with prioritisation. So, within the category of emerging security challenges, do we have a rational basis upon which to prioritise – to determine resource allocation, speed and cohesiveness of policy response? As a general rule highest priority challenges are those that threaten the survival of people and institutions. This includes climatological, nuclear, biological, health and agriculture-related challenges. Second order priority challenges could be considered to be threats that by any means (separately or in combination with others) undermine essential ways of life and the fabric of society. What might be the first and second order priorities in a list consisting of emerging rather than new security challenges?

How can we identify such emerging security challenges? Monitoring for risk is possible, even in a time of austerity. Expertise on risk monitoring does exist outside government and intelligence circles. For example, venture capitalists who seek to bring technologies to market, and reinsurance companies, which seek to calculate and mitigate risk, closely monitor commercial potential of scientific breakthroughs. As such, in principle these bodies provide analysts with an under-utilized 'early warning' or 'weak signal' indication of possible emergent threats and challenges in the near future, particularly as the time between innovation/ breakthrough and the market place is becoming shorter and shorter. In practice hedge funds often rely heavily on secrecy or information that allows them to be first-movers. Reinsurance companies, however, are keenly attuned to unknowns and catastrophic risk. Nevertheless, against such a backdrop, the analytical capacity of policy institutions to raise awareness and planning to address the known emergent challenges is lacking, never mind their ability to devise strategies for the unknown or to engage policy makers in a learning process. Given institutional, cultural, and economic constraints, appropriate partnerships that bring together experts from NGOs, think-tanks, business and academia can fill the vacuum. Such groups must be multidisciplinary, adopting collaborative approaches and employing analytical rigor to examine factual evidence with the purpose of synthesizing existing knowledge. Through deliberate reporting these groups can provide reasoned, insightful, and clear analysis that provides state actors the opportunity to deeply consider what is genuinely emerging, focus on awareness and produce better policy. In order to reduce strategic surprise, foresight efforts must be embraced.

29 July 2013

NB: The authors co-chair the newly established "Emerging Security Challenges Working Group" of the Partnership for Peace Consortium, a voluntary association of institutes of higher learning in defense and security affairs linking over 800 defense academies through a network of educators and researchers that share best practices and develop concrete solutions to common challenges. They benefited greatly from shared insights and stimulating discussions at two workshops over the last year. This paper, however, is not based on a consensus of the members of this working group, but reflects the assessment of the authors.

About the authors

Graeme P. Herd (g.herd@gcsp.ch) is a Senior Programme Advisor and Senior Fellow, Leadership and Conflict Management Programme, Geneva Centre for Security Policy. From 1 September 2013 he will be Director, (graeme.herd@plymouth.ac.uk) School of Government, Plymouth University, UK.

Detlef Puhl (puhl.detlef@hq.nato.int) is a Senior Adviser, Emerging Security Challenges Division, NATO HQ, Brussels, Belgium and is Co-Chair of the PfP-C ESC WG.

Sean Costigan (sean_costigan@post.harvard.edu or costigs@newschool.edu) teaches international affairs and technology at The New School University and is Senior Adviser to the PfP-C ESC WG.