TECHPOPS

Center for
International
Peace Operations

100 Voices on Technology & Peace Operations

Partnering for digital technology innovation

The EU and crisis management in the age of technological disruption

22 June 2020 | Dr. Daniel Fiott

International organisations are playing catch-up to the rapid development of emerging technologies and greater digitalisation, especially as these new systems and processes are being produced at a seemingly breakneck speed by a range of commercial and government actors. As of today, international actors such as the United Nations and the European Union at least agree that artificial intelligence (AI), 5G, Big Data and even quantum computing, are likely to affect every area of life in profound – if uncertain – ways. How these technological developments are likely to affect peacekeeping and crisis management is unclear.

The EU currently deploys 17 missions and operations with around 5,000 personnel in 11 countries. They face many of the same challenges as UN peace operations and, in fact, find themselves in the same operating area as the UN, for instance in Mali, Somalia, Iraq and others. In seeking to unravel and respond to the uncertainties surrounding digital technologies in peace operations that affect both organisations, a look at developments in the EU context can provide useful insights and reveal opportunities for collaboration.

EU FORAYS INTO DIGITALISATION AND TECHNOLOGY

On the part of the EU, this uncertainty has not stopped the Union from investing in technologies that can be used by civilian and military personnel. The European Commission has, for example, already pledged a percentage of the forthcoming European Defence Fund to 'disruptive technologies' and the Permanent Structured Cooperation that almost all member states have signed up to is seeing the development of unmanned systems, space-based technologies, cyber and electronic warfare capabilities.

Beyond investments, the Union is also grappling with the wider geoeconomic implications of digitalisation and its 'Global Tech Panel' is studying how technology can serve the values of the EU rather than work against them. It hardly bears repeating that the development of AI and the use of data raise a whole host of ethical concerns related to meaningful human control of technology and data protection, to name just a few. This is the reason why in September 2019 EU defence ministers met with the Global Tech Panel to discuss strategic and ethical concerns and challenges. Such discussions will inevitably inform the development of EU defence technologies and capabilities.

However, advanced technologies such as AI are already being used by the EU. For example, the EU Satellite Centre (SatCen), which serves as the Union's geospatial intelligence (GEOINT) body and provides intelligence and image analysis for the EU's Common Security and Defence Policy (CSDP), currently uses AI-enabled systems to help it more effectively map, chart and analyse satellite intelligence. As just one example, SatCen has used AI-enabled systems to help it decipher the size of shipping vessels, which, in turn, has assisted with a range of tasks such as helping to enforce arms and oil embargoes. Such technological tools could also be useful for effectively managing the vast amounts of data accrued during a crisis management mission or operation.

Despite the use of AI-enabled systems by EU CSDP bodies today, as yet there is no coherent plan for how emerging technologies and digitalisation could be used by CSDP institutions, missions and operations. Still, there is some strategic-level thinking: The European Defence Agency is engaged in studying the strategic contexts, in which certain emerging technologies could be applied, and the EU Military Staff are investing intellectual energy into better understanding what digitalisation means for EU security and defence. This reflects an awareness that it is not simply a case of detailing what technologies could be developed and used by the EU for crisis management purposes, but rather of outlining the strategic dimension in which they could be employed.

It certainly appears that emerging technologies could be used to enhance the EU's ability for data management, situational awareness, training and simulation, supply and maintenance and personnel protection and surveillance. AI-enabled systems could assist EU civilian and military planners with inventory and supply line management, and the use of Big Data could assist with resource, health and statistical management at refugee camps. There is also scope for new technologies to help with civilian-military planning and training, especially in the context of the EU's integrated approach to crises.

STAYING AHEAD OF THE CURVE

The development of technologies to meet all of these challenges points to the Union's need to ensure that it maintains information superiority during peace and crisis management operations. This, in turn, reflects growing fears that the EU might be falling behind the technology curve and that the conflict environments in which the Union is likely to deploy to in the future will be technologically congested due to the use of electronic, cyber and improvised commercially available technologies.

If the need to grasp the relevance of emerging technologies has taught the EU anything about crisis management operations and missions, it is that the relatively permissive environments that the Union deploys civilian and military personnel to are shifting into more hostile and more intense conflict zones. Indeed, part of the puzzle of ensuring that emerging technologies can assist with EU peace and crisis missions and operations is understanding how adversaries like terrorist or rebel groups can also capitalise on the proliferation of sophisticated technologies.

For example, even though a continuing challenge in crisis management is the role played by small arms and light weapons, information and communication technologies are already being exploited by terrorist groups to recruit and radicalise individuals as well as to sustain disinformation campaigns against peacekeepers and crisis managers. Moreover, it is not far-fetched to assume that that widely available and more sophisticated technologies can also be used. We only need recall how in 2018 Venezuelan President Nicolás Maduro was attacked during a military parade by two drone-borne improvised explosive devices. Such instances show how cheap and conventional technologies can be combined with sophisticated and unconventional systems.

Despite these worrying advances, however, one of the most pressing technological areas of concern for peacekeepers and crisis managers is cybersecurity. Often called the fifth domain of warfare, offensive cyber tools threaten to paralyse EU civilian and military communications and command and control (C2) channels or gain access to classified materials and IT infrastructures. Of course, one of the major challenges associated with cyber defence is the difficulty of attribution – the truth is that malicious cyber-attacks can be launched by criminals, terrorists and/or states alike. If several military experts believe that the extensive use of AI-enabled systems in warfare is five to ten years away, offensive cyber technologies are a clear and present danger that can be mobilised by numerous groups that already today possess the requisite technical know-how.

Faced with these mounting strategic and technological issues, how can an actor such as the EU chart a course that helps it maintain and extend its technological and operational credibility? Of course, financial resources and investment in technology are important and so too is a more vibrant relationship between the commercial and defence sectors – civilian firms are notoriously good at developing new technologies and applications. Yet, it is far too easy to simply say: invest, invest, invest. Instead, a key issue facing EU civilian and military crisis planners today is the need to ensure that crisis managers are properly connected and interoperable.

Indeed, any digital infrastructure employed by the EU for crisis management purposes should allow for sufficient civil-military coordination and the infrastructure must ensure an extremely high level of security for communication and C2. Given these needs, the EU is still at an early stage in the digitalisation of CSDP and an immediate task is to breed a common understanding of what digitalisation and emerging technologies mean in the context of its operations. This common understanding does not only apply to EU member states but EU institutions too – in reality, the Union has barely begun to connect all of its financial resources and existing initiatives on digitalisation, AI and emerging technologies.

TECHNOLOGY IN THE EU-UN STRATEGIC PARTNERSHIP

To zoom out of the specifics of the EU's technology strategies, and to conclude this contribution, it is perhaps worth bearing in mind that the EU represents a unique test-case for the application of emerging technologies to crisis management and peacekeeping. The Union has already stated that technologies such as AI should be used in line with its values, and so as it adopts new technologies for CSDP missions and operations partners may well be able to learn from EU actions.

In the context of the EU-UN strategic partnership, there is scope to deepen exchanges on technology and peacekeeping. In fact, at least three of the eight priorities agreed under the EU-UN Strategic Partnership could benefit from emerging technology developments (i.e. training, early warning, capacity building). In this respect, the EU and UN could usefully discuss emerging technologies and peacekeeping in a more structured manner at future iterations of the Steering Committee on Crisis Management. After all, effective EU-UN cooperation will in part be dependent on the interoperability and effectiveness of their crisis-relevant technologies.

ABOUT THE AUTHOR

Dr. Daniel Fiott is Security and Defence Editor at the EU Institute for Security Studies (EUISS). He is also a Visiting Professor at the Institute for European Studies at the Free University of Brussels (VUB) and a Visiting Lecturer at the Brussels School of International Studies at the University of Kent. The views expressed in this article do not necessarily reflect those of the European Union or the EUISS.