Ethical Dilemmas and the Future of European Defence

www.e-ir.info/2013/10/10/ethical-dilemmas-and-the-future-of-european-defence/

André Barrinha ,

e-IR has recently published a number of thought-provoking pieces (such as Daniel Fiott's analysis of the Common Security and Defence Policy and IR theory, or Tom Dyson and Theodore Konstadinides focus on CSDP limitations) on CSDP that have certainly enriched the debate on European defence. This brief article intends to be part of that discussion, by looking at the potential ethical consequences of the technological advancements in European defence, in particular the progressive use of remotely controlled vehicles, associated with the centrality of the cyberspace, all framed in a context of increasing privatisation of services and suppliers. A triple combination that is here labelled as post-modern defence.

After briefly analysing how the EU and some of its major member states are dealing with the privatisation, robotisation and virtualisation of security and defence, the article will explore the ethical challenges associated to these three dynamics.

From Private Companies to the Cyber Space: European Defence in Flux

Privatisation. From security guards to software specialists, private security and military companies are nowadays an integral component of armed forces across the world. The increasing presence of the private sphere in the military field is, to a large extent, the result of a deeply ideological shift towards the privatisation of public services, based on the belief that private agents are more efficient than public agents (Williams 2010).

European countries and the EU itself are certainly not immune to this (global) tendency. According to Elke Krahmann, "[t]he outsourcing of military support services to private companies has been one of the most notable features of the reform and transformation of European militaries in the 1990s" (2005: 280) with the UK at the forefront of those efforts. The EU's role in this area is mostly related to the regulation of these companies from a commercial point of view. Much of what applies to these security and military companies, domestically, is defined by the rules of the single market, as stated by the Court of Justice of the European Union on more than one occasion[1]. Companies that operate primarily in the military field are under the framework defined by the 1998 Code of Conduct for Arms Exports, as well as by the common actions 1999/34/CFSP (on the proliferation of small arms) and 2000/401 (related to military technical assistance). However, given that many of these business companies operate through subsidiary companies located outside Europe, their activities are often difficult to regulate and supervise by the EU or its member-states (Krahmann 2006).

In addition to regulation and supervision, the EU should also be seen as a potential 'customer' of these companies. Even though the EU does not seem particularly interested in hiring private contractors within the framework of its CSDP missions (cf. White and MacLeod 2008), the same cannot be said of its External Action Service. For example, the EU mission in Kabul hired a private security contractor to ensure its safety (Rettman 2012).

Individual member states also seem very interested in using private services. In 2010 alone, over seven thousand contractors were deployed by the UK in different missions across the world, with the UK spending £2.6 bn, corresponding to 40% of the UK military effort overseas (Louth 2012: 46). Even though these services were initially hired to undertake non-military support and management duties, they "have moved progressively towards the front line" (Krahmann 2005: 281). Germany, France and other Southern European countries seem to be much more cautious regarding the acquisition of private services in the defence field. The question is for how long.

Robotisation. It is undoubtedly clear that the progressive use of unmanned and remotely controlled vehicles have allowed (for those conducting the operations) the reduction of the human and financial costs associated with the

exercise of the war. The possibility of carrying out surgical strikes with unmanned equipment is as (or even more) effective and costs several times less than a fighter jet, making the political burden associated with war significantly lighter. As this logic expands and technology enables the development of sea and land autonomous or remotely controlled capabilities, war becomes an exercise done at a distance, without any risk of military casualties for those who undertake the operations as has been visible in the US drone operations from Somalia to Pakistan.

Europeans have been remarkably silent about the United States (US)' recurrent use of drones in counter-terrorism (Dworkin 2013). Indeed, Brussels and the other European capitals seem more concerned with the lack of military capabilities in this area rather than with Washington's target killing policy. UAVs are an increasingly more attractive option for many member states, as demonstrated by the agreement established between the UK and France for the production of so-called Unmanned Combat Air System (UCAS) (IISS 2012). However, with the exception of the UK and France, no other member state possesses UCASs.

Contrary to the use of private companies, robotics seems, nonetheless, to be a much more consensual dimension of European defence. Britain is leading the way in this field as well, with Afghanistan and Iraq providing the British Armed Forces with important lessons in terms of the usefulness of drones in combat operations (Dyson 2010). In the same vein, France-led EUFOR in RD Congo, as well as more recent operations in Libya and Mali have given Paris the clear notion of the need to further invest in this type of equipment. In that regard, France is leading the 'nEuron' UCAV project that currently involves five other European nations with the ultimate aim of constructing a prototype that could then be used by the participating countries to eventually create a European UCAS.

Virtualisation. The EU has made numerous efforts to harmonize positions across all Member States *vis-à-vis* cybersecurity, regarding it as a priority area in the European agenda (Bendiek 2012: 19). In addition to the European Network and Information Security Agency (ENISA), the European Defence Agency is making a strong investment in the sector, being involved in the development of cyber defence technologies, capabilities and in improving training for member states and European institutions. To this, we should also add the activity in this field by EUROPOL[2], the European Police College, the European Maritime Safety Agency and the External Action Service of the EU. Despite these efforts, there is still a significant gulf between member states, with some states having already defined and revised their cyber security strategies, while others are yet to develop one. Additionally, it is rather unclear how the EU and NATO will cooperate in the military dimension of cyber security.

The (New) Ethical Challenges of European Defence

The progressive centrality of the private, associated with the technological innovations in robotics and cyber space will lead to a necessary redefinition European defence. With it, there will also be significant ethical challenges, namely the issue of accountability and the risks of privatisation.

Much has been written on the lack of accountability, transparency and legitimacy of the EU's institutions, also within CSDP. Indeed, the complex institutional architecture that works in security-related issues in Brussels provides enough room for decision to be taken outside the public eye. It gets even more opaque when we have a more encompassing view of Europe's defence, including the specific policies of member states and NATO. It is a multi-layered institutional design that touches on a multitude of policies and actors that makes public control over those policies particularly difficult. Even if the processes are transparent it is often difficult to know where to look for answers. In that regard, post-modern defence only worsens this situation, by further mixing agencies departments and (public and private, internal and external security) actors and by dealing with issues often difficult to understand to the common citizen (particularly in the cyber field). This complexity is not only problematic in terms of democratic accountability, but also in terms of institutional efficiency. In the cyber security field, for instance, there has been an explosion of new and renewed institutions and centres across Europe, most of them with very limited budgets, and potential overlapping ambitions (ENISA, EDA, EUROPOL,..).

To this we can add the increasing presence of the private in what is a primordial public domain – defence. The private sector's presence has been progressively felt in Europe since the end of Cold War, as defence industries

were (partly) privatised across the continent. This came at a time in which companies offering security and military services started to blossom internationally, with Europe being caught up in the trend, even if in different degrees and with distinct levels of enthusiasm. More recently, with advances in the cyber field, companies have acquired a central role as both privileged referent objects and as guardians of the system working side by side with governments and international organisations.

Regardless of the sector, it seems clear that (post-modern) defence ministries and armed forces will increasing look towards the private sector in order to provide services and equipment that are too expensive to maintain or too complex to operate. Defence budget cuts across Europe will also contribute to the idea that private actors provide better 'value for money'; that there is no need to maintain a public service that can be better done, when needed, by a private contractor, a trend that is widely seen across government agencies in all sorts of sectors in Europe – from Education to Health. Thus, if we are to follow this path, post-modern defence will be the age of the drone and the cyber, but also the age of the private.

Conclusion

Although Europe is less enthusiastic than the US about the use of drones and the hiring of private contracts, it is unclear whether this precaution is derived from a different understanding of those issues or if, by contrast, it is merely a problem of 'evolution', with Europeans moving towards a more intensive use of these security tools and processes. However, due to its inherent characteristics, the EU offers unique conditions for the adoption of a hybrid – neither internal nor external -, apolitical, understanding of security, with little visibility in the eyes of ordinary citizens. The EU's institutional design allows security and defence policies to develop outside the public attention, between agencies and committees more or less obscure, technically justified by the complexity of policies, the same that underlie the establishment of public-private partnerships or even *outsourcing* services.

Thus, even if Europeans are not as interested in outsourcing its security responsibilities or in placing the acquisition of drones as a primary goal of its defence modernisation efforts, the institutional context in which these measures might unfold is potentially more prone to be approved outside public knowledge. In that sense, important questions should be asked regarding the relation between citizens, states and the European project.

—

André Barrinha *is a Lecturer in Politics and International Relations at Canterbury Christ Church University and a Researcher at the Centre for Social Studies of the University of Coimbra. His most recent (co-authored) article is 'Translating Europe's Security Culture' (Critical Studies on Security).* Contact: andre.barrinha@canterbury.ac.uk

References

Bendiek, A. (2012) "European Cyber Security Policy", *SWP Research Paper*, No. 13.

Dyson, T. (2010) *Neoclassical Realism and Defence Reform in Post-Cold War Europe* (Basingstoke: Palgrave Macmillan).

Dworkin, A. (2013) "Drones and Targeted Killing: Defining a European position", *ECFR Policy Brief*, available in: http://www.ecfr.eu/publications/summary/drones_and_targeted_killing_defining_a_european_position211

IISS (2013) "Chapter Four: Europe", *The Military Balance*, vol. 113 (1), 89-198.

IISS (2012) "Cloudy prospects for Europe's combat aircraft makers", *IISS Strategic Comments*, vol. 18.

Krahmann, E. (2006) "Regulating Military and Security Services in the European Union" in Bryden, A. and Caparini, M. (eds.) *Private Actors and Security Governance*. Muenster: LIT Verlag, 189-212.

Krahmann, E. (2005) "Private Military Services in the UK and Germany: Between Partnerships and Regulation",

European Security, 14 (2), 277-295.

Louth, J. (2012) “A new model army”, *Defence Management Journal*, 58, pp. 46-47.

Rettman, A. (2012) “EU to spend €50 mn on private security in Afghanistan”, *EU Observer*, 11/05/2012, available in: http://euobserver.com/defence/116224.

White, N.D. and MacLeod, S. (2008) “EU Operations And Private Military Contractors: Issues Of Corporate And Institutional Responsibility”, *European Journal of International Law*, 19, 965-988.

Williams, M. C. (2010) “The Public, the Private and the Evolution of Security Studies”, *Security Dialogue*, 41 (6), pp. 623-630.

---

[1] See rulings C-114/97 (vs. Spain) C-355/98 (vs. Belgium), C-283/99 (vs. Italy), and C-189/03 (vs. Holland).

[2] Last January, the European Cybercrime Centre (EC3) was set up within the framework of EUROPOL.

Further Reading on E-International Relations

The US Response to North Korea: The Cyber Option
EU Security Policy in the Era of Trump: A Radical Account
Implications of Brexit for the European Convention on Human Rights
Interview – Mary Kaldor
Ukraine’s Association Agreement with the EU: Acceptable Compromises and Shared H...
EU-Morocco Negotiations on Migrations and the Decentring Agenda in EU Studies
Hungary, the Barbed Wire Fence of Europe
Criminalising Search and Rescue Operations in the Mediterranean