Autonomous Weapon Systems and Risk Management in Hybrid Warfare

By Ph.d. Katrine Nørgaard, Royal Danish Defense College

Introduction:

I thank you for the kind invitation to participate in these important discussions – although I must admit, I was quite hesitant to accept, because I am not an expert in LAWS, let alone a specialist in cybersecurity. With that in mind - as an anthropologist working with military practitioners in the Danish Armed Forces, I will adopt a practice- and context oriented approach to what might be termed as "human-machine cooperative risk management".

For the purpose of this presentation, I will use the broad definition of risk management as the identification, assessment, prioritization and communication of risk to targeted audiences. And I will use the concept of cooperative autonomous networks – or hybrid networks –as interactive networks of human operators and machines with autonomous functions. Generally speaking – as has been noted by several speakers, the word "autonomous" is meaningless without specifying the task or function being automated. There are many different ways in which autonomy can be employed in military systems and any given machine might have humans in complete control of some tasks and might autonomously perform others. This is why risk management in contemporary conflicts should be seen as a context specific collaboration – or as an intelligent partnership - of humans and autonomous weapon systems, as it has been suggested by the UK representative.

Operative risk management:

First of all, it is important to consider the operative risk environment in which humans and autonomous systems perform their tasks. In contemporary asymmetric and hybrid battlefields, autonomous technologies are used to support and augment human capabilities in all domains of operation, including the physical, virtual and cognitive domains. Decisions about the specific application of weapons with autonomous functions are never based solely on the judgement of the individual warfighter, but is authorized through the military chain of command. Hence, the use of any kind of weapon is politically mandated, legally regulated and implemented through military doctrines, rules of engagement, commanders intent and

professional ethics. Moreover, contemporary hybrid warfare is characterized by a complex, adaptive and often highly integrated combination of conventional and unconventional means and activities conducted across the full spectrum of power (i.e. military, political, economic, legal, intelligence, media etc.). Thus, in the context of hybrid warfare, security issues of autonomous weapons becomes multi-dimensional. This requires the ability of cooperative human-machine teams to coordinate, evaluate and translate a nexus of highly specialized communicative codes and data streams across multiple domains of operation. Thus, the capability to detect critical cues or "events" in hybrid networks and translate them - not only to robot engineers and programmers, but also to military commanders, legal advisors, officeholders and policy makers will be key to creating high-level situational awareness and effective control systems in hybrid network battlemanagement. To echo a distinguished colleague in the panel yesterday: Continuous discretion must be applied in all domains of operation. This is why security in autonomous cooperative systems must be based on multidisciplinary thinking.

Administrative risk management

Secondly, it is important to consider the changes in the administrative risk environment, i.e. the military and governmental bureaucracies. In recent years, the political demand for a more flexible and "responsive" administration increasingly challenges the demarcation of the bureaucratic ethos and its professional criteria of legitimacy and prudence. However, the bureaucratic ethos must in important respects be unresponsive to political enthusiasms and was until recently considered indispensable to the achievement of responsible (as opposed to merely "responsive") government (Du Gay 2008:349). This consideration of the ethics of office as a moderator of political enthusiasms becomes even more urgent in the context of an accelerated and multidimensional battlespace, where the promise of quicker reaction times, or merely the fear that adversaries might develop autonomous weapon systems, could spark an autonomous arms race.

The security risk, in other words, is that the governmental and military bureaucracies are left behind by rapidly progressing and specialized technologies. With the introduction of increasingly intelligent, autonomous technologies, the boundaries between military, ethical,

political and legal aspects are becoming increasingly blurred and challenge the binary logic of the legal-administrative semantics. In other words, the administrative risk environment is characterized by ambiguous and unstable contexts and hence with legal uncertainty at a new level: "Instead of the binary distinction legal/non-legal there are oscillations between different legalities... What is legal will then often be a close oscillation between contradictory legal norms and different values and the function of predictability is challenged or changing" (Sand 2012:190). This development has been referred to as the emergence of "hybrid law". The practice of hybrid law, then, should be seen as a response to paradoxical demands in the risk environment, such as e.g. the double attribution of responsibility to individual human operators and cooperative human-machine networks.

Political risk management:

Finally, the political risk environment should be considered when addressing the security issues of autonomous weapons. Due to the complexity and the accelerated pace of the battlefield, the shortening of decision cycles and the opaqueness of networked weapon technologies, the political transparency and democratic processes are put under pressure. Moreover, war as global governance and the role of public media in hybrid battlefields make public legitimacy the central point of gravity in the political risk environment. If public legitimacy is lost, the entire military operation and ultimately government power, is put at risk. Thus, political risk management of autonomous weapons might call for a cautious "go slow approach". Especially because autonomy in military systems requires trust – which is not easily given, and is rapidly taken away if (or when) autonomous systems fail. However, at the same time, commercial interests in the development of robotic and autonomous technologies in the civilian sector combined with the prospect of adversaries customizing and using these technologies, make political decisions and guidelines even more urgent.

Conclusion:

To conclude: In hybrid battlefields, decision making and hence risk management should be seen as a joint effort of human and machine intelligence – shaping both the operative, administrative and political risk environment. It is, so to speak, an inherently hybrid affair. The military value of autonomous weapon systems lies in the benefits of the intelligent

partnership between humans and machines – not in autonomy per se. The risk however, is that transparency and political legitimacy is compromised by the opaqueness and blurring of distinctions in hybrid networks.