

Are there tactical and or strategic advantages to be expected from the use of such systems?

There is little doubt that States will make use of most advanced technologies in the full range of military, covert and intelligence operations. Advanced capabilities constitute an important element of military deterrence. They also serve liberal democracies' strive for less lethality and destruction in the battlefield. There is evidence of mainstreaming connected technologies in, and in support of, conflict. The attractiveness of these technologies comes from their (perceived) effect – reduced time between observation and response, or, in the context of 5G, reduced latency. Further considerations for employing advanced technologies include reducing the margin of human error and cost effectiveness (unreliable and expensive human cadres).

If so, is there a risk that LAWS affect existing “power balances”?

The shift in power balance is brought by the development and use of advanced technologies more broadly than just LAWS. In particular those LAWS that are both smart and connected evidence of a relatively small group of countries possessing military advantage beyond reach of most others. The main power advantage from acquiring and deployment of these weapons is also there for small and agile countries that cannot deploy large military contingencies.

Might the development and acquisition of such systems be perceived by regional neighbors as threatening?

I think this perception is mainly why we are here today. However, as witnessed by the discourse of cyber threats, the threat narrative is insufficient and often over-emphasized. The same technological advances that can be regarded as threatening also enable economic growth and social stability. The same countries that develop and deploy advanced technological weapons also argue for international peace and security. Moreover, countries are accountable under already existing international law in their development and use if such capabilities. Use of these capabilities does not happen outside of geopolitical considerations.

How would we know that users were to apply the highest degree of caution in the development and use of LAWS?

There is evidence of that happening in the cyber domain. While countries are perhaps more willing at this stage to use these capabilities in surveillance, espionage and low intensity conflict, there is little evidence of cyber attacks by State actors resulting in destruction. The very few often-cited cases are Stuxnet and Saudi Aramco (which need to be seen in context). There are, to date, no cyber attacks by State actors that have resulted in lethality. It is not because that capability is not there. The fact that something is possible does not make it likely. There is

considerable deterrence in the existing international legal regimes governing State conduct in hostilities. We should not underestimate the self-restraint that countries exercise with regard to advanced technologies.

Will it be more difficult to prevent unauthorized users from accessing those systems or unauthorized use once they become part of conventional armed forces?

While LAWS themselves might be more susceptible to arms control than, e.g. cyber capabilities, their programming and command is difficult if impossible to control and can be changed without changing the design of the weapon itself. As in deployment of most LAWS information flows from sensors and C2 will play a role, the real use and impact of these technologies will be visible after their use. Non-physical payload (AI) is attached to physical systems, which are as protected as any 'dumb' weapon systems. Safeguards could be developed that make unintentional or unauthorized use impossible.

Non-State actor acquisition of LAWS could be observed the same way that State acquisition of LAWS. While in the case of States, with very few exceptions, there is a presumption of accountable use of such weapon systems, the onus is (or ought to be) reversed in case of non-state actors. Their cyber plus nature (a physical+connected object) makes the physical objects more easily susceptible to monitoring. While non-state actors are prone to acquire such systems they are to date less able to generate secrecy systems comparable to those of States. A lot of what we know about non-State actor capabilities is through social media. Fear-based secrecy regimes have high risk of defection. Also, non-state actor modus operandi is often publicity-oriented.

Do the unique characteristics of LAWS make proliferation in application and use more or less likely?

The prospect of proliferation cannot be argued away. States ought to consider appropriate export control regimes, adequate reactions to presumed or actual uses as well as due accounting on these capabilities.

In light of increasing sophistication of military technologies, will there be scenarios where national defense might rely on such systems?

Definitely no. Or if I would have to argue yes then only as a last resort if that is technically ever possible. National defense is systemic capability. Its value and capacity are based on parallel and mutually amplifying capabilities and capability alternatives. No one weapon system is the definite guarantee to success.