Chapter 29

Promoting International Security During Difficult Times for Arms Control

Antonio Missiroli

Editor's Note: This is a transcript of Dr. Antonio Missiroli's talk. The views presented in this intervention/article are personal and do not necessarily reflect those of NATO.

Good afternoon. I owe you many thanks for inviting me to speak here today, and notably to conclude your proceedings, which is a great honour—especially as I am old enough to have learned my first (and, sadly, only) physics at school from ‘the’ Amaldi, the handbook of physics by Edoardo Amaldi that every student in Italy used back then. Also, as an Italian, being hosted in this building is a special privilege.

But I also owe you three apologies. The first one is that I am not a physicist. I am by training a boring historian and a superficial political scientist. So, please bear with my incompetence throughout my speech. The second apology is that I am not going to talk about nuclear disarmament and related issues. I am sure that throughout your proceedings you have already discussed at length, and dissected in depth, the current state of play. Addressing it would be to some extent even a little awkward on the part of someone representing NATO here. As you know, in principle NATO is not in favour of unilateral disarmament or the Ban Treaty. Therefore I could only go as far as to read some sort of official statement on the demise of the INF Treaty that would not add much to what you already know about the issue—and I do not think that you invited me here to do this.

Instead, and this is my third apology, I will try to discuss with you what else keeps us awake at night in Brussels—which is not unrelated to what you have been discussing so far. And I am saying ‘in Brussels’ because Brussels is, as you know, a city that hosts a flurry of international organizations and decision-makers and diplomats, in particular NATO and the European Union. The EU and NATO were famously said to be based in the same city but on different planets; and now, of course, the orbits of the two organizations have got ever closer, they are almost intertwined. Thus, in order to avoid collision, what we have to do is to compare notes, cooperate

A. Missiroli (✉)
North Atlantic Treaty Organization, Brussels, Belgium
e-mail: missiroli.antonio@hq.nato.int

with and talk to one another. So what I am trying to relay is a set of concerns that occupy us all over there. And it is about the evolving strategic and security landscape at large, characterized as it is by increasing strategic competition, at both state and non-state level, globally as well as regionally. It is also characterized, and I'm sure you have discussed that, by a general weakening of the multilateral world order that goes from trade arrangements to arms control agreements and that seems to be happening ever more often.

What I would like to focus on in particular is the impact of technology on all this. Technology, in principle, is both a boon and a bane and, right now, we probably are in between two industrial and technological revolutions. One is the ICT revolution, so to speak, that is arguably still underway while we are probably transitioning already towards the next step in that revolution, which will be characterized by artificial intelligence, 5G technology, quantum computing and all that. We have started to realize only recently that, after enjoying all the benefits of the past or ongoing industrial revolution(s), we are now also starting to feel the sting or realize the 'dark side' of all that. We are just beginning to acknowledge the risks and the threats that it has also generated. And nowhere is that realization more acute than among security experts.

Let me give you a few examples. Take terrorism, which is very much in the minds of people in this part of the world as well as across the Atlantic. With the onset of ISIS, the Islamic State, terrorist actions in the Euro-Atlantic space have increased, and terrorist groups now use technology in a very effective way. In particular they use cyber space for propaganda and recruitment, for fund-raising as well as for operational purposes (a few months ago, for instance, the *New York Times* reported on the way in which militias use Whatsapp to coordinate their actions in Tripoli). But they also use 'physical' tools like drones, unmanned vehicles. You may have read that a couple of weeks ago an oil refinery in Saudi Arabia was attacked by a 'swarm' of drones, apparently carried out by Houthi rebels supported by Iran. In early 2018 a Russian military base in Syria was also apparently the target of a swarm of drones. Maybe the Middle East is a favourable ground for this kind of operations because there are large ungoverned spaces and big infrastructure is concentrated in small spaces. But perhaps it is not unconceivable to see drones operating even in urban environments, in our cities. You may remember that, less than one year ago, Gatwick airport in the UK was basically brought to a halt for two days right before Christmas by two drones that nobody has yet identified. The potential for harming entire communities is indeed enormous, especially if terrorists groups can load drones (that are easily accessible, available and operable) with CBRN agents or even improvised explosive devices.

Or take what we call cyber-attacks. A cyberattack is cyber against cyber, basically. There has been a spectacular increase in cyberattacks in the past few years, especially in 2017, when two major malware campaigns (WannaCry and NotPetya) affected critical infrastructure inside Europe and beyond, including hospitals in the UK and commercial shipping across the world. Malicious cyber activities occur on a daily basis, even routine incidents could easily escalate and be used to damage critical infrastructure: energy (including nuclear energy plants), transport, communication

and also finance. The recent Nuclear Posture Review by the United States also highlighted the fact that cyber means could be used to disrupt and disable command and control systems for nuclear warfare. As you know very well, the first every cyber-attack was Stuxnet, launched against Iran in 2010–2011. Disabling the other side is part of the game, but there is also a wider risk of disruption and loss of control we all have to be aware of. Less than one year ago, Russia's attempt to hack into the website of the Organization against the Proliferation of Chemical Weapons (OPCW) in The Hague was discovered and exposed. And, in that particular case, the international community called out Russia for what it was doing.

This is an area in which the spectrum of potential hostile actors is wide and huge: from the so-called 'hacktivists' to the proverbial 'kid in the basement', from criminal gangs to terrorist groups, up to state sponsored actors: we call these APT (Advanced Permanent Threat) and most of them are located in China, Russia, North Korea and Iran. In some of these countries ministries are also directly involved in coordinating and directing all this. Hackers can steal our credentials, they can steal our money, they can steal industrial secrets, but they can also steal critical military information and carry out all sorts of online espionage. They can also exfiltrate data and perform large scale sabotage—all of which, in turn, could also be(come) part of a phased operation leading to overt conflict.

Insofar as these operations are covert actions for an intelligence operation, they are not even against international law as we know it: international law does not address espionage as such although law enforcement, especially at domestic level, can of course help address this issue. These operations are comparatively low cost and low risk, high impact and high reward; they are easy to deny, because tracking back algorithms rarely brings certainty in terms of attribution; they are difficult to detect, too, and difficult to deter. It is almost impossible to aim at absolute deterrence in this particular field, simply because the offence is at a structural advantage. They have the advantage of space and time: they can attack anywhere anytime as the attack surface in the digital world is virtually infinite.

Finally, and this is probably more of interest to you, traditional arms control and non-proliferation mechanisms cannot really work in this domain. Firstly, the legal framework at international level is very weak, as there is no such thing as the International Atomic Energy Agency in Vienna or the OPCW in The Hague to regulate this particular field. Secondly, traditional mechanisms of inspection, verification and disposal are not really applicable, if anything because the 'weapons', so to speak, range from a laptop to a code: not only cannot they be conclusively detected or destroyed, they can also be easily recreated. And, thirdly, there is no state monopoly on the legitimate use of code (as opposed to the legitimate use of force) and the threat actors in this domain are often beyond state authority or control.

It is also worth recalling that the kind of effects and the damage that these 'weapons' can create are not as visible or painful as physical effects. Therefore, it is also more difficult for the international community to mobilize against them, because there is no resulting moral or visual horror comparable to that produced by nuclear weapons. There has been no single case so far in which a cyberattack

has brought so much damage that the international community was prompted to act against the perpetrators.

Even confidence building measures—as those traditionally applied in the WMD domain—do not really work. The Organization for Security Cooperation in Europe in Vienna has tried to engage its members in a dialogue to this end but with modest results, in part because some of the actors who have capabilities in this domain feel they have an edge and do not want restrictions that may erode it.

Last but not least, there is what we now call hybrid. By nature and definition, a ‘hybrid’ is a combination of different types of elements or, in this case, actions: military and non-military, covert and overt. It is what Russia did in Georgia in 2008 or in Ukraine in 2014. Interestingly, however, the original use of the term ‘hybrid’ in the context of warfare dates back to the conflict between Hezbollah and Israel in Lebanon in 2006, when Hezbollah used a multiplicity of different means—from hi-tech to very primitive tools, from urban guerrilla to conventional techniques against Tsahal, the Israeli Defence Force. That also included what we call the ‘weaponization’ of social media—something that is now probably familiar to you as citizens, something we have seen happen over the past few years in our democracies, on both sides of the Atlantic. Basically, ‘hybrid’ techniques entail and encompass a mix of disinformation, destabilization, disruption, deception, subversion, coercion—along a spectrum that ranges from espionage to sabotage. And virtually all are, now, cyber-enabled.

We have seen all this already, of course, especially during the Cold War. But what is indeed different now is the use of modern technology, which makes it much faster and more effective. Technology acts as a multiplier and accelerator and, potentially, as a game changer (also) in this field. First of all, it is changing the balance of power(s) worldwide, notably between the ‘haves’ (which are not necessarily the usual suspects, or at least not only) and the ‘have-nots’. But it is changing also the internal balance of power in our own societies. You are surely familiar with the notion of the ‘digital divide’: some people have access to these technologies while some are excluded or are even victims of these technologies. An additional risk is represented by the fact that some of the ‘haves’ may not be guided by the same values and principles that we are, thus raising the concerns about their future use of such new and potentially disruptive technologies—at least as long as there is no international legal framework to constrain and restrain their behaviour.

The UN is doing a lot of work in this particular domain, especially in terms of soft law and codes of conduct. As you know, there is ongoing work in New York on the so-called lethal autonomous weapons systems, and a group of selected governmental experts is working (again) on cyber-related issues. The general state of international relations, however, appears hardly favourable for any major multilateral breakthrough, at least at this stage. Therefore, our expectations have to be modest. The emphasis is increasing on what we call ‘responsible state behaviour’: since it is impossible to entirely deter these kinds of operation, it is important to be able to identify what they should *not* aim at. In other words, since it is impossible to limit the ‘weapons’, it should be advisable to limit at least their ‘targets’.

Yet the new technologies are not simply changing the balance of power(s)—they are also altering the balance of players, mainly because their peculiarity is

that they are mostly privately generated, privately owned and privately operated. Cyberspace is the most relevant case in point. Most of the technologies we are talking about have been developed in and by the private sector. That was not the case with nuclear, chemical, biological or radiological weapons: they were state-generated and therefore largely controllable through interstate negotiations. The new ones are not being developed privately but the time required to hit markets is much shorter than in the past. Although most of these technologies are intrinsically dual-use, more often than not market considerations trump security considerations (that applies even to our mobile phones). Therefore, we are confronted with a scale of risks and vulnerabilities that certainly was unconceivable before. Take Google, Facebook, Amazon, Microsoft or Apple, but also Huawei, Alibaba or Tencent. These are the new superpowers—and nothing comparable to the so-called ‘military-industrial complex’ of decades past.

The next industrial or technological revolution is about 5G technology, artificial intelligence, machine learning and quantum computing. That is the next stage in the Great Transformation. As American futurologist, Roy Amara, famously coined a law whereby we tend to overestimate the short-term impact of new technologies and to underestimate their long-term impact, and we may indeed be confronted exactly with this phenomenon now. We tend to be extremely worried about what may happen 3, 4, 5 years from now with the introduction of IG technology, but we may not be sufficiently foresighted to see what may come in 20 years from now. Another one, Alvin Toffler, also said that the future always comes too fast, and in the wrong order. In other words, we do not know what may truly happen not only five but especially ten or twenty years from now—as much as we surely did not see coming a few years ago what is on now. But we have to be sufficiently lucid to try and seize the opportunities that the new technologies offer. In the field of human health it is quite evident that artificial intelligence, for instance, offers a range of unprecedented benefits, especially for an aging mankind. But there are other areas in which we tend, instead, to be much more concerned about their possible effects. You are certainly familiar with the discussions on ‘killer robots’, ‘Terminators’, ‘Robocops’ and so on and so forth—especially, as I said, since there are rising powers that are not constrained by the same rules of the game or moral principles that we have developed and would like to maintain and foster. Therefore, mitigating and managing the risks is the other side of the coin: seizing the opportunities and exploiting the potential benefits, yes, but also mitigating and managing the risks.

However, the name of the game is no longer just deterrence, which probably cannot have the same meaning as the type of strategic and absolute deterrence that we have seen at work since 1945. It is also resilience—and resilience supported by education. Explaining to people what can be done with the new technologies, but also what should not be done is essential. Even countering the manipulation of public opinion that is happening with the weaponization of social media requires a lot of education—as well as a healthy information landscape, that is not always a given.

As Western and democratic societies, we suffer some limitations in this field. Externally, we do not necessarily want to replicate or imitate the behaviour of those who want to do us harm, we do not want to do tit-for-tats—an approach that somehow constrains our response options. And internally, of course, we do not want to limit

our own freedoms in order to combat disinformation or disruption: we do not want to limit free speech or restrain ownership of media or industrial assets. So our very nature of open societies—our declared strength—may come to represent, at the same time, a potential vulnerability and a structural weakness.

My last point is that any effective action in this field must be a coordinated one, a team effort: at national level (whole of government as well as whole of society), at transnational level (especially between like-minded countries), and at international level (between and across multilateral and regional organizations). As these hostile activities—terrorist, cyber and hybrid attacks—know no geographical borders and no jurisdictional boundaries, we have to be able to do exactly the same: build trust, cooperate and exchange information between and across nations, organizations, public and private actors.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.