P.A.L. Ducheine, Vilnius 23 May 2024

Learning From Legal History to Prepare the Future in the Domain of Technological Developments

Ladies and gentlemen, dear participants, I'd like to thank the organisers for having me here. As ever, it's great to participate in the Society's congresses. Back in 1999, as a young major in 1GNC, I was ordered by my chef, the then treasurer, to attend a seminar in Brussel. After that experience, I volunteered for the Lillehammer Congress (2003), and only missed three since that time. Along the road, I met many colleges, and some of them have become dear friends. So: I encourage the young lawyers to keep attending the events, and above all, I call upon the older lawyers, the chefs, to follow my chef's policy: please stimulate the youngsters to join and participate in the society.

After this 'commercial', I'd like to start with two waivers. First of all: my mother tongue is Flemish, not English. Please bear with me.

Secondly, and more importantly, I must confess today I'm operating outside my comfort zone.

Despite my initial education in civil engineering, and as lawyer trained by inter alia prof Terry Gill, I presume I'm supposed to feel comfortable with the present topic. However, history is not my speciality. Neither is the history of IHL. Those who know me, will say that I'm a pragmatic lawyer, but above all a military scholar.

Hence, I feel uncomfortable.

Actually, and here the presentation starts, this is the second time in two year time that this actually happened. The second time in relation to cyber warfare that is. Two times uneasiness in relation to history and cyber warfare.

How is that? The explanation, and actually todays presentation centres around going back and forth in time. Let me explain.

Let's go back to early March 2022. About a week or two into the war (RF-UKR). I received a phone call from a journalist who worked for the Dutch journal "Kijk". The journalist asked me to reflect on my earlier interview to the same journal, back in 2017 (related to my chair in cyber warfare at the Netherlands Defence Academy). The journalist asked me explicitly to reflect on the title of the 2017 interview: "the next war will take place in cyberspace (too)". Initially they proposed it without the "too". But lawyer-ish, I forced them to add the "too". In retrospect, that proved fruitful.

Because the journalist asked me whether the 2017 prediction had materialised. I had not. That is: not at first glance. I had to admit that. It was the start of two surveys.

The first survey: was it valid, in 2017, to come up with a prediction of this kind at all?

And the second survey, if yes, where was the cyber side of the war? Was the prediction wrong, were cyber attacks absent? Or was it just that we couldn't "see" them? If so, why was that?

Together with my research group, we concluded that the prediction was a valid one. We came up with three arguments.

- By 2017 States had already demonstrated their willingness to use cyber attacks in wartime: especially the RF had launched hacks in December 2015 and 2016 causing massive black outs in UKR. Moreover, it also launched NonPetya against UKR's (VAT) taxation services, causing massive collateral damage to *inter alia* the shipping company Maersk, with massive financial losses as a result. By the way, also Russian companies like Gazprom and Rosneft suffered from the attack.
- In addition, by 2017, some 30 other states had started to set up cyber commands within or adjacent to their armed forces.
- But most importantly, once societies become an informational one, and social interactions increasingly become digitally, eventually, the "niche" social interaction called war will become digitalised as well. So: cyberwar will inevitable come.

So survey one was concluded: the prediction was a valid one.[1]

Survey two commenced.

After intense research over more than a year, and like many others, we made four observations.[2] The spoiler is: There was indeed a cyberwar going on "too", but it looked different than we anticipated: less hacking (at least visible or notable), and much more soft cyber or cyber-enabled influence operations.

Looking back on this research and actually, looking back on this war: These facts are now history. Even today's events have become history as of tomorrow. History, so the past, but nevertheless very relevant. For various reasons. Operationally as well as legally.

Operationally (relevant as we lawyers should understand what we're advising about).

Each and every time (yesterday's) history reveals new methods or means of warfare, we can learn from them. Learn from the ingenuity and creativity of engineers designing new techniques. And learn from commanders employing these newly invented means (AI,

---

[1] See P.A.L. Ducheine, Peter B.M.J. Pijpers & K.L. Arnold, "The Next War Would Be a Cyberwar, Right?", in: T. Sweijs & J.H Michaels (eds.) Beyond Ukraine - Debating the Future of War (Hurst Publishers, 2024), pp. 85-106.

[2] See K.L. Arnold, Peter B.M.J. Pijpers, P.A.L. Ducheine & P. Schrijver, "Assessing the Dogs of Cyberwar: Reflections on the dynamics of operations in cyberspace during the Russo-Ukrainian war", in: M. Rothman, S. Rietjens & L. Peperkamp (eds.) Reflections on the Ukraine War (Leiden University Press, 2024), pp. 231-256. Open access: https://library.oapen.org/handle/20.500.12657/87676.

malware, drones) and use them in a new fashion. In this way new means (tool/instruments/weapons) of warfare have been developed, new addressees (targets) came to the fore, new vectors to deliver the weapons on target were used, and above all new concepts of warfare have been conceptualised. Think of drone warfare, but of course also of cyber warfare.

Legally (as this is our bread and butter) new techniques, enabling new means and methods of warfare, are even relevant.

There are various elements to that notion. Let me cover two of them. One short, one more in depth.

Short: The use of means and methods often resulted in subsequent additions to IHL. Often after the horrific effects of the weaponry became clear and the costs of the suffering proved too high (you can think of the ban on the use of chemical weapons after WWI, the ban on antipersonnel mines after the wars in Africa and Afghanistan (in the last century), cluster munition).

However, and more in depth, the use of new technologies such as cyber capabilities require instant deliberation. First of all, because article 36 AP1 requires a review. Secondly, because it is in the overarching interest of legitimacy as a principle of western military conduct, to ascertain the legitimate use of the new technology once it is vetted (after the 36 AP1 review just mentioned). For that reason, each and every time, the application of new means and methods have to be (re)considered in light of existing IHL.

The latter enterprise, can be extremely difficult. Difficult, but nevertheless necessary. The sometimes heard call for new protocols or additions because there's new technology being used, is – in my view – premature and probably unnecessary. At least premature as long as we haven't done our job as legal advisors properly. In that respect it would be wise to read the law first, or the manuals, before proposing additional rules.[3]

Admittedly, going through the endeavour to check how new technology aligns with IHL is a stressful job when time is scarce. Thankfully, this was foreseen by people like professor Mike Schmitt in the field of cyber warfare, or people alike in the area of space operations. Thanks to their efforts, we can fall back on Manuals that have been prepared to support practitioners: operators, policymakers, and lawyers when time is sparse.

However, were not there yet. Even with the Tallinn Manual at our disposal, there's still work to be done.

Therefor I'd like to take you back to my 2017 prediction: the next war will take place in cyberspace. The next war is today. And yesterday too. It is history. And it is the future.

[3] RT(*)M: Read the (*) Manual!

With the aid of the Tallinn Manual, (and the statements of various States afterwards) we have to learn from recent history and continue to do our homework on the application of IHL in the light of recent observations.

Let me name five observations (and I'm pretty sure some people in the room will have an idea on the answers to these questions). Or perhaps, I should start reading the Tallinn Manual too (again). And just as a reminder: there's more legal issues at stake than IHL's alone.

1. What to make of the thousands participants in the war and in the wider conflict from all over the world: the hackers who answered Ukraine's call to join its IT Army. What is their status? Are they DPIH? What about the orders their follow: who's accountable for the targeting decision made upon which they act? How about their (domestic) criminal responsibility? What if their action drags a state into the war? How about neutrality (as if that isn't an issue in itself).
2. And what about the people in the combat zones that hand in information that is use in subsequent targeting? Or the ones that develop the app to enable this? Do we consider this a war sustaining effort? And what are our – shared views on that in multinational operations?
3. What about IT firms? I'm not just talking about the firms and services that follow sanction regimes (by the way: as we learned yesterday, it's an addition to the work of legal advisors (legads), at least in UKR). And I'm not specifically referring to those companies and services that have been forced by RF legislation to stall operations. I'm particularly worried by the crucial role the firms proved to play in enabling communication in general, Command & Control (C2) in particular, in delivering Cyber Threat Intelligence, in enabling modern days conduct of business.
4. Fourth: how to deal with the vast amount of influence operations. Not just the legitimate ones (in our western view), but also the malicious ones directed at our home countries? Are they – together with acts of sabotage – the frontrunner of the grey zone war that some of our policymakers like to see?
5. And finally: where are we now. In 2024. Seven years after I thought that we would be moving into an information society. In which data is the new oil, the holy grail? Do we continue to take the conservative view as laid down as a black letter rule in the Tallinn Manual? Where the majority of the international group of experts considered an object to be something tangible (see art. 52(2) AP1)? And where damage for some was only at stake when hardware had to be replaced (after an attack)? And how about the principle issue of what constitutes an attack (as defined in article 49 AP1) in itself?

Yesterday we learned from dr. Gurmendi Dunkelberg, that the constructs we use, “were build today”. I’d like to add: “today, based on yesterday’s knowledge, experiences and interpretations”.

With this in mind, I’d like to conclude be referring to the recent dissertation by Mrs Raissa van den Essen. She accepted the challenge to look into the relationship of targeting non-tangible items (data) by researching the relationship between attack, object-military objective and (collateral) damage. Although cyber operations are here today and tomorrow, she looked at yesterday’s concepts. She researched and analysed the background and development over time of the three concepts.[4]

Thus she learned from history of IHL in order to understand today’s and tomorrow’s war. And she learned it whilst there was plenty of time. The luxury we’re missing right now.

In Deutsch: es gibt viel zo tun, fangen wir an (in English: there’s a lot of work to be done, let’s get started).

[4] R.S. van den Essen (2024) *Targeting data in armed conflict - Interpreting international humanitarian law’s fundamental notions of ‘attack’, ‘object(ive)’ & ‘damage’ against the effects of cyber operations* (diss. University of Amsterdam), via: https://hdl.handle.net/11245.1/41bfa8e2-e6c3-4f2a-9689-39ff838efcfc