Dual-use technology regulation

The regulation of dual-use technology in a data driven digital world

On April 21, 2021, The European Commission's proposal to regulate artificial intelligence (AI) involved the ban of numerous of its possible applications. The fact that a new European Union legislative process commences with the ban of certain aspects of a technology is audacious. Yet it is often not the tool that is problematic, but the usage made out of it. The fact that technology should not be used for certain purposes is perfectly legitimate in a democratic society. Nonetheless, technology is neutral. Specifying what purposes should be avoided for each and every type of technology hinders readability of human rights safeguards to put in place within digital activities.

The stem of the European Commission's concerns is the lack of understanding of risks related to this new technology and the numerous scandals of AI use in military contexts (Pasquale 2020). The fact that AI has dual civil and military uses deserves to be taken into account. As defined by the European Commission, "[d]ual use goods are products and technologies normally used for civilian purposes but which may have military applications" (European Commission, 2021)[1]. As AI is a dual-use technology should it be added to the Wassenaar Arrangement regulating the uses made of certain dual-use technologies? Interestingly, it has not been the case so far. Maybe the legacy regulatory framework is flawed or too slow to integrate new technologies when they emerge.

The European Commission's definition narrows the dual-use tool definition to "goods" - but the digital era has accelerated the trend towards the polarisation of wealth on the tertiary sector. Economies have changed, we should probably think less in terms of goods only and more in terms of goods and services accompanying them. More broadly, the ethos of dual-use tech regulation is to recognise and protect from the risks of certain tools being developed for civil purposes, while they would become potent weapons in a conflict. The rise of weaponised digital tools could seemingly lead to the same approach to analogical dual-use weapons. Yet although the root problem bears common features, should dual-use technology regulation apply to digital technologies? In order to echo this interrogation the state of dual-use technology regulation shall first be presented in order to seize its spirit (I). Next the regulatory framework will be confronted to the new realities of the digital revolution (II), thereby enabling to outline potential regulatory optimisation (III).

[1] European Commission. 2018. "Dual-Use Trade Controls." Retrieved May 9, 2021. (https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm)

I) Dual-use technology regulation

A. Sources of dual-use technology regulation

First and foremost, studying the source of the present Wassenaar Arrangement provides useful insight into the evolution of its purpose.

Dual-use technology regulation finds its roots in the post World War II world. Countries of the Western bloc led by the United States (U.S.) sought to embargo certain goods produced by the so-called Comecon countries, gathering socialist countries and led by the Soviet Union. Although the exact date on which the Coordinating Committee for Multilateral Export Controls (CoCom) was created is still surrounded by secrecy, the primary goal of this tool was to become an anti-communist export control network (Yasuhara 1991). With the end of the Cold War the purpose of an export control tool targeted towards a restricted group of stakeholders due solely to their political ideology became anecdotal. Instead, it was the need to recognise the sheer destabilising power of certain technologies to serve civilian and military purposes that was relevant, and a growing concern considering the advancements of chemical and nuclear research. The CoCom therefore ceased to exist in 1994. Until its replacing tool would enter into force the list of embargoed goods was retained by former nations states members until the birth of its successor, the Wassenaar Arrangement.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (hereafter the Wassenaar Arrangement) was adopted in 1996. It currently counts forty-two member states, including Russia, Turkey and the US. It has achieved its ambition to become a legal tool bringing diverse countries around the same negotiation table. Today the Wassenaar Arrangement encompasses a wide-ranging scope including arms, their components (like fissile material) as well as computing and telecommunication technologies (Wassenaar Arrangement, 1996 and 2013). Decision-making takes place on majority vote, and it does not provide veto powers to any of its members (Fidler 2015). The Wassenaar Arrangement is built on an inclusive licensing model, as opposed to its predecessor with a closed off embargo strategy. The current policy is one of non-legally binding international reflection on how to mitigate destabilisation tools, together. It relies on a multilateral export control regime aiming to promote international security through transparency, responsibilities, and best practices (Michel *et al.* 2013; Wassenaar Arrangement 1996).

That said, despite having become a global shared arena for critical dual-use technologies conversations, in the last decade the Wassenaar Arrangement has proven to create frictions when attempting to adapt to essential evolutions of societies.

B. A failed attempt to harness surveillance abuses

Due to growing international surveillance abuses concerns, the Arrangement's members deemed it urgent to update the list or restricted tools. Indeed, reports of Western surveillance technologies deployment for human rights abuses in countries like in Bahrain and the United Arab Emirates (UAE) (CitizenLab 2012), Turkmenistan (CitizenLab 2013) and Libya (EDRI 2013) were closely following each other. As a result, in 2013 the Wassenaar Arrangement list was amended to incorporate computer intrusion software and IP network analysis technologies (Garnick 2014).

Overall the 2013 evolutions have been met with considerable skepticism as stakeholders were not clear whether highly problematic dual-use technologies like 0-days were finding themselves regulated (Fidler 2015), while certain critical activities such as cybersecurity research could be hampered by the conservative wording of the reform (Bratus *et al* 2014).

Skepticism was most notable in the U.S.. In the aftermath of the Arrangement's reform the U.S.'s Department of Commerce Bureau of Industry and Security (BIS) proposed in 2015 a broadened version of the 2013 reform. Its proposal was to require a license before exporting, importing and/or sharing of systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software including network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices (U.S. Department of Commerce, Bureau of Industry and Security 2015). *Prima facie* this proposal therefore prohibited the sharing of vulnerability research if one did not process a license to do so (Galperin *et al* 2015). Civil society organisations as the Electronic Frontier Foundation (EFF) rose awareness about the unintended risks born by the proposed national law reform, and campaigned for the private sector to join them in their call to denounce the reform's pitfalls. In fact the very reform of the Wassenaar Arrangement list was deemed unadapted to digital activities, and therefore any adaptation of the reform to U.S. law would carry unacceptable competition, human rights and research risks too dire to contemplate. The proposal was therefore abandoned and U.S. diplomates were invited to impress on the Wassenaar Arrangement participants that the surveillance technologies dossier needed reworking (Galperin 2016).

On the other side of the Atlantic, the European Union incorporated the changes by passing a 2014 Regulation (European Commission 2014) modifying its first Regulation of 2009 adapting the Wassenaar Arrangements into EU law. EU legislation helpfully expressly exempts antivirus technologies from its scope[2]. Unfortunately it is still unclear to what extent research is exempt. This could have a chilling effect on researchers, or void the regulation of its essence. Indeed, if research was part of its scope and researchers still worked normally, the legislation looses all credibility. Legislative adaptation of the EU's framework to the 2013 additions to the Wassenaar list is still in force.

Divergences between the U.S. and the European transpositions since 2014 are striking. Such considerable dissensions rooted in the first attempt of the Wassenaar Arrangement to cover software technologies are a bad omen for the continued tackling of human rights abuses facilitated by malicious software. As Ambassador Griffiths to the Wassenaar Arrangement Secretariat explained at a 2017 meeting of the Organization for Security and Co-operation in Europe (OSCE), although certain operator-controlled surveillance tools are covered by the arrangement, software itself is not (Griffiths 2017). The interpretation that surveillance software in itself is not covered in the Wassenaar Arrangement could be seen as undermining the overall effectiveness of the arrangement.

Yet the legislative gap between the Arrangement's participants since 2013 potentially illustrates a fracture at a more fundamental level. Maybe the legacy dual-use technologies paradigm is irrelevant

[2] The EU Regulation provides that ""Intrusion software" (4) means "software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following […]" and specifies that "monitoring tools" include antivirus technology.

to the dual-use technologies emerging from what certain coin the information revolution (Floridi 2010). What characterises a revolution is that is disrupts pre-established norms that used to be stable.

II) A data driven paradigm

The paradigm based on which the Wassenaar Arrangement is built is that certain tools or their components can at any time be used for military purposes instead of civilian ones. Yet this way of categorising certain digital tools is not relevant, and crucially fails to address the radically new trend of data and personal data mining.

A. Loss of relevance of the legacy regulation

Building on the criticisms raised against the U.S.' attempt at infusing the 2013 Wassenaar amendments in national legislation, assessing the analogies between items of the Arrangements does lend itself to bewilderment. Historically a dual-use item would for instance be a gun. Civilians will legitimately need it to hunt, police men and women may need it in high risk missions. Yet sheer accumulation of such items will concern the neighbouring countries as the purpose for which these guns are used could drift a few years later and lead to a ferociously armed country posing an immediate threat to peace for other countries. Yet applying the same thinking to a 0-day does not seem relevant. The very destabilisation power of 0-days is tied to their essence. A 0-day will be a highly potent weapon as long as it remains a 0-day - that is, as long as it remains a vulnerability unknown by the entity or the community maintaining the code it is meant to exploit. Once the exploit is known its threatening dual-use potential is drastically reduced, if not completely. For instance, the EternalBlue (Sanger *et al* 2017)[3] 0-day integrated in the WannaCry code provides an interesting case study. It is fair to say a former 0-day can still remain a dangerous weapon online due to erratic patching of servers, even in critical infrastructures with guilty cyber risk management like the British National Heath Service (NHS) (Townsend *et al* 2017)[4]. Yet as opposed to guns, it is possible to provide means to mend the vulnerability exploited - to patch it, so to speak.Once patched the impacts of the attack may not be mended, but the threat itself entirely disappears. A pistol or a knife remains dangerous with time. A 0-day becomes outrightly harmless in a patched environment.

[3] "The cyber-attacks on Friday appeared to be the first time a cyber weapon developed by the N.S.A., funded by American taxpayers and stolen by an adversary had been unleashed by cybercriminals against patients, hospitals, businesses, governments and ordinary citizens". Sanger D. E. and Perlroth N. 2017. "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool" *the New York Times.*

[4] For the sake of accountability it must be highlighted that the absence of basic cybersecurity risk management of the NHS servers by Sophos in 2017 cannot be downplayed. For political reasons the server maintenance contract was ended and another solution was never put in place. The fact that no other health system around the world experienced similar failings gives an idea of the scale of the failing. Leaving critical infrastructure to run unmaintained code is outright criminal in the digital era - the fact that the cybersecurity advisor of the NHS has not seen its accountability publicly debated is a tragedy. This point deserves to be highlighted because 0-day accumulation certainly is an issue, but leaving a national health system exposed to any kind of cybersecurity risk is a fault to a radically different level.

Besides, and at a more concerning level, business models have evolved in conjunction with the realisation that data analysis can generate continuous service improvement material. The current trend is not anecdotical - digital service providers increasingly offer services to civilians and to the military (Gasler 2020; Fang 2019)[5] that continuously analyse user's behaviour in oder to improve. In fact, such services are not even limited to civilians and the military. They have additionally been deployed in ethically questioned law enforcement (Sherman 2020) and humanitarian (Parker, 2019) programs, despite the outrage of international civil society (Privacy International *et al* 2020). A common pattern among these service providers is the fact that they proclaim to not process personal data. This point is critical and vastly problematic for two reasons.

B. New unprecedented risks

Firstly, accumulating knowledge on human unconscious behaviour and biases for profit purposes raises profound ethical questions. The growing cognitive dissonance caused by the large scale harvesting of behavioural patterns from humans, mostly obtained without prior informed and free consent, has been developed by Shoshana Zuboff in 2020 (Zuboff 2020). In many ways Zuboff asks the right questions before concluding that one of the keys of surveillance capitalism is the unfettered harvesting of what she coins "behavioural surplus". The Covid-19 crisis has added to the somewhat pathetic irony created by the race of companies towards monetised human behaviour patterns when it became public that the Palantir company had contracted with the British NHS to help it analyse its data for the price of one symbolic pound. A for-profit actor chose to support an entire country's national service, in a historical moment where failure could be a reputational swan song, for one pound. Presumably the value Palantir will get from the analysis of the data is worth the reputational risk, time and money it will have invested. Similarly, and although the United Nations (UN) paid a high price to use Palantir tools, having a company seed funded by the CIA generate highly monetizable "fraud"[6] behavioural patterns drawn at the detriment of genocide victims in need (Parker 2019) is ethically dubious, to say the least.

The second reason why companies processing unprecedented amounts of human's data while claiming it is anonymous is concerning because it frees them from fundamental rights compulsory due diligence. This aspect has a plethora of detrimental subversive implications that will be discussed. Yet beforehand one foremost consideration: is it even anonymous data? A safe answer should be no, due to emerging research on complex data sets (Hern 2019) and because anonymisation processes may always be reversed by future technologies (European Data Protection Supervisor 2021). Last but not least, given these technical unknowns the answer should be no because some of the individuals whose data was harvested are the most vulnerable on the planet - the degree of precaution they should be afforded should be the highest. Ironically so far the UN

[5] See "Out of all the companies that surfaced in Tech Inquiry's research, Microsoft stood out with more than 5,000 subcontracts with the Department of Defense and various federal law enforcement agencies since 2016. Amazon has agreed to more than 350 subcontracts with the military and federal law enforcement agencies, like ICE and the FBI, since 2016, and Google has more than 250, according to Tech Inquiry's analysis." Gasler, April. 2020

See also the Intercept article "GOOGLE continues investments in military and police AI technology through venture capital arm", by Fang, Lee. 2019.

[6] Although the World Food Program contracted with Palantir to improve the tracking of fraudulent behaviours there is no reliable source indicating that big data analysis on migrants is particularly efficient to understand and curb fraud.

World Food Program (WFP) has only had privacy impact assessments that highlighted overwhelming concerns as to the risks created to individuals[7].

In addition, claiming data processed is only anonymous data is extremely concerning as it *de facto* frees for-profit entities from fundamental data protection requirements and principles, such as the obligation to deploy technical and organisational measures ensuring cybersecurity, data minimisation and purpose limitation principles[8]. By the same token, if data is "anonymous" it frees one from assessing the risks its processing might create for individuals. This may be the crux of the issue as not having to conduct assessments means no audit trail can be requested by regulators for accountability purposes. On top of that, the notion of assessments has been considerably reinforced in the EU since 2018. When processing activities may create high risks for individuals, EU law now requires the conducting of a Data Protection Impact Assessment - an exhaustive analysis of implications, remediation measures and an iteration process preventing to commence activities until risks have been lowered.

Altogether the concerns surrounding companies exploiting behavioural surplus are high from a human rights perspective - but benefit from a lack of technical understanding at international policy level. Nonetheless the fact that the human behaviour extracted more or less without informed consent from often distressed individuals might benefit the military-industrial complex is disturbing. Especially in a context where countries increasingly reinforce their military capacities with what they refer to as contractors, but are often old fashioned mercenaries (Usborne, 2014).

In a personal data driven digital society the legacy notion of dual-use items has lost its relevance. It may be illustrated by a mundane observation. On the European Commission's website one finds the "dual-use" notion only associated with goods, and this will be in the "trade" section of the website only. Times have changed. As highlighted above, today most of monetised activities are not goods but services. Moreover, reducing the monitoring of dual-use to a purely trade related debate sends a clear signal. Either the accountability of legal entities whose purposes encompass civil and military ones is disrupted, or it is clear that offering a service to civilians to feed their data to algorithms and artificial intelligence will remain a juicy business model. Probably a proper surveillance capitalism model. A subsidiary remark on the matter is that digital services contract increasingly include a clause that the data processor that is the service provider reserves itself the right to extract anonymous data from their customer's data, for their own purposes (Zuboff 2020). Often to train algorithms. This trend may be the visible tip of the iceberg showing a market trend to gather anonymised data on users, just in case, influenced by the success of companies like Google who built their success on big data. This phenomenon may echo an observation of Zuboff - when the majority of economic actors act unethically it can become unaffordable for an ethical one to do the opposite (Zuboff 2020) as all their economical ecosystem is aligned on the unethical model.

Nonetheless this gloomy portrait does not have to be a fatality. It may just be the sign that solutions are elsewhere. For risks to be harnessed and accountability to be rebuilt, laws must create documentation requirements and enforcement mechanisms. The current overall erosion of trust

[7] Not published - Data Protection Impact Assessments (DPIA) done in 2018 and 2019 concluding to high risks. The DPIA done in 2019 was done on SCOPE, the World Food Program platform collecting data whose data analysis in supported by Palantir. The data collected includes biometric data of genocide victims from the age of 5.

[8] These guiding principles can be found in the General Data Protection Regulation as well as a growing number of countries' legislation.

online vis-à-vis States and private businesses may open an opportunity to reset a legislative paradigm tailor made for the challenges of today.

III) Regulating legitimate purposes

Means to legislate at the international level exist and can create cohesion. International law is built on one ambivalence: there are two spheres where actors evolve. The private sphere, where for-profits are regulated, and the public one, rather focusing on States and their duties and rights vis-à-vis the private sector. Yet the new paradigm presented above may call for multiple adaptations, not only regarding how dual-use technologies are understood and defined, but also how international law adapts to global evolving needs. To this day there have been numerous initiatives to prompt for a rethinking of how dual-use technology is harnessed. These initiatives will be reviewed before we move to assessing how to best meet the emerging needs.

A. From Wassenaar to Vienna

One of the most frequent dual-use technology examples today is artificial intelligence. In 2019 Microsoft released its HoloLens 2 glasses, a product embedding artificial intelligence features into a pair of glasses to augment reality. HoloLenses 2 were initially presented as designed for civilians. Later that year it was made public that Microsoft had signed a 479 million dollar contract with the U.S. Department of Defence, leading to tensions within Microsoft (Wong 2019). Here the data of civilians might participate to hone the product, as a result of individuals buying the product, while the company is open about its work with the military. Most importantly, the company's CEO, Brad Smith, published a public statement to support "the country's civil and democratic processes" and recognise "the important new ethical and policies issues that artificial intelligence is creating for weapons and warfare" (Smith 2018).

The way Mr Smith approaches the question acutely resonates with the cybersecurity adage that the main vulnerability sits between the chair and the keyboard. Dual-use of digital technologies is not purely a trade question. Nor only a war studies one. It is a multidimensional one, that needs to be robustly rooted in ethics and democratic values such as accountability. Regulation is possible, and in fact absolutely necessary, but on a holistic level. As rightly highlighted by Zuboff (Zuboff 2020), it is not acceptable that humans' behaviour can be mined and used to build for profit strategies sold to the highest bider. The solution is not technical but political.

The Wassenaar Arrangement, aside from the critical fact that its list is utterly unreadable, is built to be reactive to new technologies, instead of built in a technology neutral fashion grounded in ethical principles that would always be applicable. It cannot be a useful beacon in the night to drive decisions, as history shows. How is it possible that Western countries needed their private sector citizens to sell tools that would threaten the life of journalists in unstable countries (*Op. Cit.* CitizenLab; EDRi) to feel there needed more conversations about these tools' risks? Surely upholding human dignity and the right to not be victimised by a government could have been expected as part of regulated due diligence from for-profits. A tool requiring human rights scandals to timidly improve, in a non-binding fashion, is a terrible one.

The Wassenaar Arrangement was an timely regulatory initiative, but it is non binding, reactive and poorly written. As seen above, its wording actually creates fragmentation between countries' adaptation. Most importantly, it diminishes what dual-use tools conversations should be about today. These tools can no longer be regulated only for competition or unfair militarisation advantages. Human rights stakes are too high. What is acutely needed today is a holistic binding tool grounded in human rights principles to be technology neutral, while putting the onus on the choices made by legal entities like for-profits or governments. No need to reinvent the wheel. For instance, the humanitarian sector's "do no harm" principle is a simple yet sound one. Guiding principles such as the "do no harm" or the accountability principles are future proof beacons.

International law treaties can be binding means for a few countries and/or international organisations to agree on a certain issue. Conventions, on the other hand, are a sub-type of treaties meant to bring countries together on broad overarching challenges. As a result certain conventions are binding tools to regulate treaties, like the Vienna Convention on the Laws of Treaties (VCLT) of 1969, that guides the interpretation of international treaties. Hence earning itself the nickname of Treaty of the treaties (Aust 2006). Other examples are the Geneva Conventions meant to set the building blocks of basic duties and rights in war and humanitarian aid contexts.

B. A new Public International Law order

In 2015 the Microsoft corporation started advocating at the UN for a Geneva Conventions inspired convention to curb the detrimental effects of state-sponsored attacks[9]. Its efforts were included in the 2015 United Nations Group of Governmental Experts (GGE) report. In July 2017 the GGE report failed to reach consensus due to certain contentious points like the application of humanitarian law (Sukumar 2017). Aside of the GGE, the Shanghai Cooperative Organization (SCO) members[10], comprising China and Russia, have expressed a different vision of the future of cybersecurity and internet governance in two versions of a Code of Conduct[11]. It is interesting to note that this Code's opening paragraph relates to dual-use technologies with both civilian and military applications. The need for better regulation solutions is therefore openly stressed. The Code was certainly presented to the UN with the ambition to gather consensus and advocate for internet freedom and sovereignty of states over multilateralism. Overall the text tackles globally shared concerns, yet as rightly highlighted by the CitizenLab, the paramount power associated with state sovereignty raises considerable human rights concerns and the Code is "dominated by intelligence, national security, and regime stability imperatives" (McKune 2015). As of today, the SCO's non-binding Code has not been adhered to by a significant amount of countries. Nevertheless this political stance should not be taken lightly. Today the SCO's members represent half of the world's population (Nazarbayev 2005).

[9] Source?

[10] SCO website - http://eng.sectsco.org/

[11] The first version of the code was published in 2011. Here is the second 2015 version: https://eucyberdirect.eu/content_knowledge_hu/2015-sco-international-code-of-conduct-for-state-behaviour-in-information-security/
Here is a version of the Code highlighting its evolutions between the 2011 version and the 2015: https://openeffect.ca/code-conduct/

More generally, for civil society actor Access Now, states' actions still demonstrate the need for an international agreement[12]. Russia has been accused of interfering in national elections by Germany, the U.K., Ukraine and the U.S. (Shane and Isaac 2017). President Putin has blamed the U.S. for WannaCry (Roth 2017). The pandemic itself has brought a swarm of accusations from EU Member States of fake news from China and Russia to shake the trust of EU citizens in their leaders (Scott 2020). The report of the Panel[13] recommends to pursue the international effort to regulate online activities in a multi-stakeholder "systems" approach[14]. Concordantly the report recommends "the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action."[15]

Unfortunately, the report does not make recommendations on the crucial need for the power of private entities to be recognised as vectors of destabilisation technologies. Yet they are overwhelmingly potent ones. Accountability mechanisms must be put in place to infuse human rights in their decision-making, policies and processes. The report does highlight that human rights are the same online and offline, but harms and redress mechanisms are absolutely not sufficiently studied or known in the digital space. The report barely scratches at the surface of the problem by stating that women and minorities must be included by all stakeholders.

So far the Global Commitment on Digital Trust and Security does not seem to be a project any actor or institution works on or towards. It probably does not matter since the report's recommendations do not tackle the growing cognitive dissonance caused by the unregulated mining of human behaviour data for obscure and unlimited purposes. To tackle the ethical dead end, non-binding niche tools that are unreadable and fall in the trap of technicalities is a disgrace to humankind. What the international community needs is a binding ambitious public international law tool, a convention, with rights enforcement mechanisms. Such convention should be elaborated following a multi-stakeholder process and could create space for treaties on aspects of technologies that require additional rules, such as automated decision making features. It must aim to be holistic, by using technology neutral principles such as do no harm, accountability, purpose limitation and proportionality. Microsoft's initiative is extremely relevant, but only covers state sponsored activities. Hopefully the landmark stance of Dr. Zuboff, documenting the emergence of "behavioural surplus" grabbing business models has made the regulatory gap blatant. Her work and the abuses observed detailed above require an ambitious digital rights convention enshrining that states are no longer the most powerful international law actors - private companies are too, and must be regulated in the same UN convention.

Conclusion

[12] "Despite the ideological and process differences, recent state action demonstrates the need for international agreement.", p. 9 of "A Digital Rights approach to the tech accord and the digital Geneva convention" report, Access Now. 2018.

[13] Report available online - https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf

[14] Recommendation 5B of the 2019 report.

[15] Recommendation 4 of the 2019 report.

To conclude, although the regulation of dual-use technology applied to the digital era requires new regulatory strategies, *the spirit of dual-use technology regulation remains legitimate*. Hoarding the proliferation of destabilising subversive technologies is critical for a better world. Yet the legacy regulatory tool, the Wassenaar Arrangement, is not relevant for digital tools and services. Indeed, dual-use digital technology requires a holistic regulatory binding tool encompassing all relevant international public law actors.

The adapted regulatory tool should be an international binding one with a broad membership and ambitious scope - an international convention. Since 2015 the idea of a broadranging Digital Geneva Convention emerges. Such convention, setting fundamental principles to impose safeguards in the digital society at all times, needs to infuse the behaviour of relevant actors with core guiding human rights and democratic principles. *C*urbing nascent trends that rightfully raise concerns among civil society, scholars and the wider public will not be done by issuing licenses to companies or states. The burden of showing one acts as a responsible international law actor must be pushed on the most powerful actors, for them to become accountable. This is particularly true today where around the world governments grapple to provide their citizens with decent critical infrastructures. It is no longer acceptable to expect a country to invest plethoric amounts of money to demonstrate the human rights dangers caused by a certain company.

On a personal note, I chose to study subversive technologies because my previous experience had showed me that it will be easy for policy makers to be trapped in a never-ending and exponentially quickening path of evolving technologies. It is easy to feel overwhelmed and irrelevant in the face of new technologies - how they work and their need to be harnessed to minimise harm. I was dearly hoping that this course would lead me towards refusing to be reactive and instead peacefully look at evolving technologies from the lens of future proof principles. The analysis of dual-use technologies regulation has proven to be the allegory of that intellectual journey. Its spirit is legitimate, but it fell in the trap of setting technology specific measures for new pieces of technology, leading to uncertainty and fragmentation. Whereas policies grounded in ethics and fundamental rights will remain relevant. In fact, technology neutral principles centred on the protection of human rights and our environment must be the cornerstone of subversive dual-use technology regulation. The need to be an expert in a certain emerging technology in order to be relevant to discuss the ethical limits it must not cross is chimerical and detrimental in the long run. I am immensely grateful for having had the opportunity to hone my thoughts reach this conclusion.

Bibliography

Access Now, 2018. “A Digital Rights approach to the tech accord and the digital Geneva convention” report. *Access Now*. Retrieved May 12, 2021 (https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf)

Aust, Anthony. 2006. "Vienna Convention on the Law of Treaties (1969)". *Max Planck Encyclopedia of Public International Law*.

Bratus, Sergey, *et al*. 2014. “Why Wassenaar Arrangement’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It”. *Computer*

Science Department, Dartmouth College. Retrieved May 20, 2021 (https://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf)

CitizenLab. 2012. "Backdoors are Forever: Hacking Team and the Targeting of Dissent?" *The Citizen Lab*. Retrieved May 7, 2021 (https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/)

CitizenLab. 2013. "For Their Eyes Only: The Commercialization of Digital Spying" *The Citizen Lab*. Retrieved May 7, 2021 (https://citizenlab.org/2013/04/for-their-eyes-only-2/)

CitizenLab. 2015. "An Analysis of the International Code of Conduct for Information Security". The Citizen Lab. Retrieved May 1, 2021 (https://citizenlab.ca/2015/09/international-code-of-conduct/)

EDRi, Edrigram newsletter n°10. 2013. "Amesys – Complicity in torture: surveillance tech export control needed". *EDRi*. Retrieved May 11, 2021 (https://edri.org/edrigramnumber10-10amesys-complicity-in-torture/)

European Commission. 2014. Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. OJ L 371, 30.12.2014. Retrieved April 9, 2021 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1382)

European Data Protection Supervisor (EDPS). 2021. "10 misunderstandings related to anonymisation". *EDPS website*. Retrieved May 14, 2021 (https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf)

Fang, Lee. 2019. "Google continues investments in military and police AI technology through venture capital arm". *The Intercept*. Retreived May 15, 2021 (https://theintercept.com/2019/07/23/google-ai-gradient-ventures/)

Fidler, Mailyn. 2015. "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis." *A Journal of Law and Policy for the Information Society,* 11(2):405–83.

Floridi, Luciano. 2010. "The Cambridge Handbook of Information and Computer Ethics". *Cambridge University Press*.

Galperin, Eva *et al*. 2015. "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?" *Electronic Frontier Foundation (EFF) website*. Retrieved April 23, 2021 (https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation)

Galperin, Eva *et al*. 2016. "House Grills State Department Over Wassenaar Arrangement" *Electronic Frontier Foundation (EFF) website*. Retrieved April 23, 2021 (https://www.eff.org/deeplinks/2016/01/house-grills-state-department-over-wassenaar-arrangement)

Gasler, April. 2020. “Thousands of contracts highlight quiet ties between Big Tech and U.S. military”. *NBC News*. Retrieved May 15, 2021 (https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171)

Granick, Jennifer. 2014. “Changes to Export Control Arrangement Apply to Computer Exploits and More”. *Center for Internet and Society, Stanford Law School*. Retrieved April 14, 2021 (https://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more)

Griffiths, Philip. 2017.“Presentation to the OSCE Forum for Security Cooperation (FSC),” May 31, Vienna.

Hern, Alex. 2019. “'Anonymised' data can never be totally anonymous, says study”. *The Guardian*. Retrieved May 13, 2021.

Michel, Quentin, Sylvain Paile, Maryna Tsukanova, and Andrea Viski. 2013. *Controlling the Trade of Dual-Use Goods - A Handbook*. PIE Peter Lang.

Nazarbayev, Nursultan. 2005. Welcome declaration to open the SCO summit of 2005

Pasquale, Frank. 2020. “‘Machines set loose to slaughter’: the dangerous rise of military AI”. *The Guardian*. Retrieved April 22, 2021 (https://www.theguardian.com/news/2020/oct/15/dangerous-rise-of-military-ai-drone-swarm-autonomous-weapons)

Privacy International and No Tech For Tyrants. 2020. “All roads lead to Palantir” report. *Privacy International website*. Retrieved May 2, 2021 (https://privacyinternational.org/report/4271/all-roads-lead-palantir)

Parker, Ben. 2019. “New UN deal with data mining firm Palantir raises protection concerns”. *The New Humanitarian*. Retrieved May 14, 2021 (https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp)

Roth, Andrew. 2017. “Russia’s Putin blames U.S. cyberspies for global hacking wave”. *The Washington Post*. Retrieved May 1, 2021 (https://www.washingtonpost.com/world/russias-putin-blames-us-cyberspies-for-developing-virus-used-in-global-hacking-wave/2017/05/15/a01602e0-3967-11e7-8854-21f359183e8c_story.html)

Sanger D. E. and Perlroth N. 2017. “Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool” *the New York Times.* Retrieved April 14, 2021 (https://www.nytimes.com/2017/05/12/world/europe/)

Scott, Mark. 2020. “Russia and China push ‘fake news’ aimed at weakening Europe: report”. *Politico.* Retrieved April 22, 2021. (https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/)

Shane, Scott and Isaac, Mike. 2017. “Facebook to Turn Over Russian-Linked Ads to Congress“. *The New York Times*. Retrieved May 1, 2021 (https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html?mcubz=1&_r=0)

Sherman, Natalie, 2020. “Palantir: The controversial data firm now worth £17bn”. *The BBC*. Retrieved May 3, 2021 (https://www.bbc.co.uk/news/business-54348456)

Smith, Brad. 2018. “Technology and the US military”. *Microsoft blogs*. Retrieved April 4, 2021. (https://blogs.microsoft.com/on-the-issues/2018/10/26/technology-and-the-us-military/)

Sukumar, Arun. 2017. “The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?” *Lawfare blog*. Retrieved May 7, 2021 (https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well)

Townsend M. and Doward J. 2017. “Cyber-attack sparks bitter political row over NHS spending”. *The Guardian.* Retrieved April 12, 2021 (https://www.theguardian.com/technology/2017/may/13/cyber-attack-on-nhs-sparks-bitter-election-battle)

United Nations, GGE report. 2015. UN General Assembly Resolution A/RES/70/237. Retrieved May 3, 2021 (https://dig.watch/un-gge-report-2015-a70174)

United Nations, High-Level Panel on Digital Cooperation. “The Age of Interdependence” report. *UN website*. Retrieved April 22, 2021 (https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf)

US Department of Commerce, Bureau of Industry and Security (BIS). 2015. “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items”. Retrieved April 24, 2021 (https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-11642.pdf)

Usborne, David. 2014. “Blackwater mercenaries face justice for bloodbath in Baghdad that caused 14 civilian deaths”. *The Independent*. Retrieved May 3, 2021 (https://www.independent.co.uk/news/world/americas/blackwater-mercenaries-face-justice-bloodbath-baghdad-caused-14-civilian-deaths-9701810.html)

Wassenaar Arrangement, Secretariat. 1996. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Founding Document*. WA-DOC (17) PUB 001.

Wassenaar Arrangement, Secretariat. 2013. *Public Statement 2013 Plenary Meeting of Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. Vienna.

Wong, Julia Carrie. 2019. “'We won't be war profiteers': Microsoft workers protest $480m army contract”. *The Guardian*. Retrieved April 5, 2021 (https://www.theguardian.com/technology/2019/feb/22/microsoft-protest-us-army-augmented-reality-headsets)

Yasuhara, Yoko. 1991. "The Myth of Free Trade: The Origins of COCOM 1945–1950". *The Japanese Journal of American Studies,* 4: 127–148. Available online (https://web.archive.org/web/20040730220532/http://wwwsoc.nii.ac.jp/jaas/periodicals/JJAS/PDF/1991/No.04-127.pdf)

Zuboff, Shoshana. 2020. “The Age of Surveillance Capitalism”. *Profile Books*.