Advanced Technology – Advanced Terror

An Interdisciplinary Study on Disruptive Technology and The Rule of Law

*Zénó Suller**

Abstract

Today, we are witnessing a technological and scientific boom never seen before, whose changes and effects we cannot foresee. However, it is certain that technology will also be used for malicious purposes and violence. This study focuses on the threats advanced technology may pose to national and international security. It analyzes how disruptive technology may undermine social trust, public order and public safety. How will these innovations be used by terrorists and how will technology challenge existing legal concepts under international law? This paper seeks to answer the question whether international law can provide protection against individuals' or states' misuse of technology targeted against safety and freedom. Can the international community enforce the rule of law on the international level? Will advanced technology challenge our concepts on the contested notion of state terrorism and the legality of intervention against such states? Is the international legal regime resilient enough to cope with these new threats? Finally, this paper also covers the possible solutions of cyber-countermeasures and cyber-sanctions.

Keywords: disruptive technology, terrorism, rule of law, intervention, international criminal law.

1. Introduction

Technology has always been the main fuel and material base of almost all human development and progress. Inventing the wheel or the plough may not seem much like advanced technology now, but at the dawn of human history these simple inventions profoundly changed the way of life, ensuring more stability and well-being. Following the industrial revolutions, technology provided comfort and safety for more people than ever before. This higher level of welfare also facilitated social progress, emancipation, and a desire for more equal and just political and economic structures.

However, technology is not always to the benefit of all. Technology has long been seen as a threat to humanity. All eras had their own misconceptions about

* Zénó Suller: Ph.D. candidate, Pázmány Péter Catholic University, Budapest.

doi: 10.5553/HYIEL/266627012023011001017

new gadgets, machines, or ways of production. Trains or cars were regarded with suspicion and fear. Even introducing electricity to households caused panic for some. Unfortunately, concerns are not always unfounded.

When new weaponry emerges, it can hardly be seen as an improvement to our lives. However, as is often the case, the value of an invention cannot be considered simply black or white. When the first transplantation of a human kidney was successfully carried out in 1954 it was a huge achievement with an unimaginable potential to save lives. On the other hand, as the technology and the know-how became widespread, trade in organs emerged and people have been kidnapped and slaughtered for their organs to be sold at the black market. Splitting atoms to release vast energy was supposed to solve the problems caused by our energy-thirsty lifestyle. Yet, the underlying brilliant physics theory was turned around into creating and deploying nuclear weapons, indiscriminately destroying cities with their entire populations. More recently, cryptocurrency has been developed to protect the value of money, to stabilize exchange rates and prices, side-stepping corrupt governments and greedy banks. Now, cryptocurrency is the number one choice for speculation, financing terrorism and implementing transactions between criminals. In what follows, this study will introduce some areas of technological development which are most likely to cause significant risks to national and international security.

2. Technological revolution and its dangers

2.1. Some Examples of Disruptive Technology and Their Possible Misuse

Disruptive innovation as a concept was first used in the field of economics. The notion refers to the tendency that a smaller business entity which lacks the vast infrastructural, financial and professional background of an established company may successfully challenge the markets of big players by introducing a revolutionary innovation, mainly technology.[1] In the field of international law and security, disruptive technology has a similar meaning. Actors, be they individuals, or groups with relatively limited resources can disrupt social systems, such as electricity networks, energy plants, financial cyber centers, or even governmental portals. In this domain, however, disruptive technology has a broader meaning than its economic counterpart in the sense that in the hands of the 'big players' they can be even more dangerous. Disruptive technology may be used by the state to intimidate its citizens, to control and monitor them, in short, to restrict their liberties. Evidently, technology may also be used by terrorists to carry out deadly attacks. In this sense, disruptive technology therefore means the malicious use of technology.

Disruptive technology may include several fields of technological development: 3D printing, drones, robotics, cryptocurrency, social media, deep fake, Big Data, Machine Learning, digital piracy, AI, or the dark/deep web. In what follows, I present some ways in which such innovations may be misused.

1 Clayton M. Christensen *et al*., 'What Is Disruptive Innovation?', *Harvard Business Review*, December 2015, at https://hbr.org/2015/12/what-is-disruptive-innovation.

2.1.1. 3D Printing

3D printing is a fascinating innovation. Professionals refer to 3D printing as additive manufacturing (AM). The main point is that an AM machine prints the material in 3D in a way that the typically melted or liquified substance is layered on itself. Therefore, the layers are added on previous layers of substance – hence the name: additive manufacturing.[2] This fact alone renders AM a very economical way of production as well as a creative one, since one can create complex forms which would have been impossible without this technology.[3] But AM is much more than a reasonable method for producing commercial items. It enables ordinary people to create a huge array of objects at home. There is no need to have a complete production line or massive energy resources. Moreover, in case one has the desired item's blueprint, one may print the exact copy of already existing, already produced and well-tested product.[4] Thus, the blueprint is another equally important element of AM technology besides the additive injection of the substance. The blueprint makes the printed products reproduceable. This file resembles and almost replaces the traditional know-how of production. Instead of assembling a whole factory with all the necessary machines and workflow, a build file can simplify the process enabling everyday people to use just this build file to reproduce the item.[5] But this value has its dangers.

Cody Wilson from Texas printed a perfectly functional handgun with his hobby 3D printer.[6] As a human rights activist campaigning for the right to carry weapons he generously shared his design. He uploaded the blueprint on the internet so now everyone can make the same exact copy of the Liberator. Soon, even metal guns were printed,[7] as well as bullets.[8] However, them being produced from plastic or metal, it is still easier and more reliable to get weapon from the black market. This may be the reason why printed guns have not yet been used in terrorist attacks.[9]

Terrorist attacks are often carried out by lone perpetrators – at least within the EU.[10] Since terrorist networks are in most cases of global nature, ISIS or al-Qaeda could recruit personnel as well as organize and carry out actions with lone assassins.

2 Major Stephen Hummel & Colonel F. John Burpo, *Small Groups, Big Weapons: The Nexus of Emerging Technologies and Weapons of Mass Destruction*, 2020, p. 10, at https://apps.dtic.mil/sti/pdfs/AD1100991.pdf.

3 Marco Fey, *3D Printing and International Security: 'Risks and Challenges of an Emerging Technology*, Peace Research Institute Frankfurt, 2017, p. I, at www.researchgate.net/publication/317175090_3D_Printing_and_International_Security_Risks_and_Challenges_of_an_Emerging_Technology.

4 Id. p. 1.

5 Adam Brown *et al*., 'Legal Aspects of Protecting Intellectual Property in Additive Manufacturing', in Mason Rice & Sueejet Shenoi (eds.), *Critical Infrastructure Protection X*., Springer, 2016, p. 64.

6 Gerald Walther, 'Printing Insecurity? The Security Implications of 3D-Printing of Weapons', *Science and Engineering Ethics*, Vol. 21, 2015, pp. 1435-1436.

7 John Newman, 'Solid Concepts Uses Metal Additive Manufacturing to Build a Gun', *Digital Engineering 247*, 8 November 2013, at www.digitalengineering247.com/article/solid-concepts-uses-metal-additive-manufacturing-to-build-a-gun/.

8 Alexis Kleinman, '3D-Printed Bullets Exist, And They're Terrifyingly Easy To Make', *HuffPost*, 23 May 2013, at www.huffpost.com/entry/3d-printed-bullets_n_3322370.

9 Noelle van der Waag-Cowling & Louse Leenen (eds.), *Proceedings of the 14th International Conference on Cyber Warfare and Security*, ICCWS 2019, p. 106.

10 *Terrorism Situation and Trend report*, Europol, 2021.

doi: 10.5553/HYIEL/266627012023011001017

For such terrorists, even a relatively simple handgun may be sufficient especially if printed at home with the help of a shared blueprint file.[11] To substantiate the devastating potential of home printed plastic guns, some Israeli journalists have downloaded a weapon build file from the Internet and printed, then assembled the parts into a functioning gun. To simulate an assassination, they pointed the gun to the head of the Israeli prime minister at a shooting distance.[12] Naturally, they did not fire the weapon, but they have proven the point that these cheap and easy plastic guns may be dangerous after all.

This may raise some questions of public safety. The legal framework governing weapons in Europe is built on the premise that the use of armed forces and firearms in general is the monopoly of the state. The state therefore strictly regulates the production, distribution and ownership of weapons requiring a special license.[13] If the blueprints for guns are freely accessible on the Internet and the weapons can be produced by way of AM, the whole regulatory system becomes ineffective. As for the infrastructure, AM provides several opportunities. Printed guns can be produced from plastic or ceramic material. Needless to say, metal detectors and gates screening for weapons are useless in this regard.[14]

The real breakthrough brought about by AM is that it affords users the ability to print multiple materials alone or together. Hence, besides plastic, AM can print metal as well as rare alloys, ceramics, glass or even living tissues or bacteria.[15] Indeed, an AM machine not only prints glass or metal, but potentially several materials combined.[16] This way, it is not only easier to produce carbon or Kevlar but it is possible to create completely new artificial materials as well, such as metallic glass, graphene, or boron nitride.[17] In addition, AM can produce items in huge dimensions as well as in nanometers; nanotechnology and bio-robotics have incredible potential for development with AM.[18] Graphene for instance is regarded as – *inter alia* – a promising material for weapons of mass destruction as it is extremely thin, yet incredibly strong with better thermal conductivity than any known metal.[19]

Another key concern is that AM can print tissues, bacteria, or even chemical substances.[20] Synthetic biology can build on this exact feature: it is a form of biological engineering creating new biological structures or artificially modifying

11 Trevor Johnston *et al*., *Additive Manufacturing in 2040: Powerful Enabler Disruptive Threat Corporation*, RAND Corporation, 2018, at www.jstor.com/stable/resrep19917.

12 Lazar Berman, 'Journalists print gun, point it at Netanyahu', *Times of Israel*, 4 June 2013, at www.timesofisrael.com/journalists-print-gun-bring-it-to-netanyahu-speech/.

13 Johnston *et al*. 2018, p. 13.

14 Fey 2017, p. 21.

15 Id. p. 4.

16 Tian Chen *et al*., 'Integrated Design and Simulation of Tunable, Multi-State Structures Fabricated Monolithically with Multi-Material 3D Printing', *Scientific Reports*, Vol. 7, 2017, Article no. 45671.

17 Fey 2017, p. 27.

18 Thomas Campbell *et al*., *Could 3D Printing Change the World? Technologies, Potential, and Implications of Additive Manufacturing*, Research Report, Atlantic Council, 2011, p. 7.

19 *Cf*. Fey 2017.

20 Hummel & Burpo 2020, p. III.

existing ones, thereby adding specialized functions to living organisms.[21] This field of science specializes in redesigning certain organisms to equip them with new characteristics.[22] The first recorded example for successful synthetic biology was in 2002, when scientists artificially created poliovirus in a laboratory.[23] The public was shocked and horrified.[24] This research substantiated that for cell proliferation, and hence for creating a new or a previously existing virus, there is no need for a parental genome. Researchers have created the poliovirus purely from its chemical components by building up oligonucleotides.[25] This means that one does not need the original virus for viral propagation. It should be noted, that these oligonucleotides are DNA segments synthetically made from chemical components.[26] No wonder scientists have realized that this amazing achievement yields a potential threat of bioterrorism.[27] AM technology along with synthetic biology can pose serious security threats, since it offers a rapid, simple and cost-effective process for developing biological weapons.

Now that the potential threats have been identified, the question arises whether AM challenges the current legal system, *i.e*. does it disrupt the defence systems of the law? Evidently, the international ban on ABC weapons[28] remain in effect. This means that should AM and synthetic biology enable states and non-state actors to develop new biological, chemical weapons, or indiscriminate weapons of mass destructions, the contemporary legal framework can provide protection through treaty law which prohibits certain weapons, customary international humanitarian law or the *jus cogens* norms of public international law. However, it is worth noting that the contemporary legal regime is based on the idea that these weapons are developed, stored and deployed by states.[29]

As far as home printed guns are concerned, we may conclude that terrorism is still a crime under national legislation and there is strong regional and international forensic and judicial cooperation between the states in this respect. As such, the necessary substantive and procedural norms are in effect. However, the enforcement of these norms through implementation may be less effective, as investigation and detection of home printed weapons to be used for terrorism may be more difficult.

21 *New Directions, The Ethics of Synthetic Biology and Emerging Technologies*, Washington D.C., 2010, p. 2, at https://bioethicsarchive.georgetown.edu/pcsbi/sites/default/files/PCSBI-Synthetic-Biology-Report-12.16.10_0.pdf.

22 *Synthetic Biology*, at www.genome.gov/about-genomics/policy-issues/Synthetic-Biology.

23 'Traces of Terror: The Science: Scientists create live poliovirus', *New York Times*, 12 July 2020, at www.nytimes.com/2002/07/12/us/traces-of-terror-the-science-scientists-create-a-live-polio-virus.html.

24 Id.

25 Eckhard Wimmer, 'The test-tube synthesis of a chemical called poliovirus', *EMBO Reports*, Vol 7, Special Issue, 2006, p. S4.

26 *See* at www.thermofisher.com/blog/behindthebench/what-is-an-oligo/.

27 Wimmer 2006, p. S5.

28 *Cf*. 1977 Geneva Conventions Protocol I; 1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction; UN Security Council Resolution 1540(2004); 1967 Outer Space Treaty.

29 Hummel & Burpo 2020, p. 1.

doi: 10.5553/HYIEL/266627012023011001017

2.1.2. Drones

Drones are excellent examples of the democratization of technology. Drones are unmanned aerial vehicles (UAV), small pilotless aircrafts.[30] Their colloquial designation, drone, comes from the fact that these small aerial machines make a low, buzzing noise.[31] Drones are everywhere. Today, UAVs are commercialized and almost anyone can buy and fly them, typically without the need for special licenses or significant monitoring and control by the state. The lack of comprehensive regulation poses legal uncertainty in several fields. UAV technology for instance may be used by terrorists to carry out attacks against the civilian population.

UAVs *per se*, even without weaponry or special equipment may pose a significant threat to the safety of air traffic. Namely, drones may form a swarm if programmed and controlled together as one entity. Such a swarm may easily force a plane to land or to crash simply due to the fact that they resemble a flock of birds flying through the air corridor.[32] As of yet, hobby drones are less advanced and they cannot fly at such heights or may be controlled as a swarm. Nevertheless, it is safe to state that this may change very soon.

Even hobby drones, however, are easy to equip with all sorts of dangerous loads. For example, a camera mounted on a drone could be used by terrorists for surveillance and monitoring. In the framework of a terrorist attack against the civilian population, an UAV with a camera enables perpetrators to monitor the allocation and the movement of the security guards and the police force, or to identify the best place to target an explosion with a dense mass and few exits for maximum destruction. Or, following the ISIS method, massacres may be recorded and broadcasted live for propaganda use. And these are only the possible uses of a camera! Terrorist attacks are usually committed in crowded public places and events. Drones may increase the effectiveness of surprise attacks in case they are equipped with explosive substances. This may help perpetrators eliminate or at least mitigate the typical pitfalls of classic terrorist attacks. Historically, most significant pitfall was that the perpetrator almost always had to 'sacrifice' their life. In case the action was carried out by handgun, hijacking or suicide bombing, the terrorist either had to die in a kind of suicide mission or be caught and arrested immediately and prosecuted. Before, it was challenging and risky to get through security checks, or to get close enough to the targeted person or location to activate a deadly weapon. The perpetrator had to remain calm and unsuspicious, had to be 'brave' enough when the critical moment arrived. All these factors present as risks. Risk for the success of the mission, and risk for the terrorist. Where it is the UAV that carries the weapon or the bomb, the terrorist attack is no longer a personal suicide mission. The drone is quick and agile, it can access almost all open spaces and it is not even suspicious. It may be quite easy to observe, but nowadays, drones are a part of public events, be it a protest, a carnival, a public ceremony or a sports competition. UAVs may therefore easily reach the critical spot and carry out the

30 Junyan Hu & Alexander Lanzon, 'An innovative tri-rotor drone and associated distributed aerial drone swarm control', *Robotics and Autonomous Systems'*, Vol. 103, 2018, pp. 162-174.

31 *See* at https://dictionary.cambridge.org/dictionary/english/drone.

32 Hu & Lanzon 2018, p. 13.

mission without the physical presence of any of the terrorists. This latter element may pose the highest risk in the future. Namely, that this way, terrorists may carry out an entire attack without even leaving their homes. The action does not require the suicide of the perpetrator and there is a real chance that the drone will either perish completely or leave the location before authorities can track it. Therefore, carrying out the attack is less risky for the terrorist and if there is less to lose and at the same time, a greater chance of a completed and successful mission, terrorist may be even more inclined to commit such crimes.

2.1.3. Social Media and Machine Learning

Social media may seem as if it were beyond the scope of modern technology and it may also appear that it does not generate new threats to the physical safety of people. Nevertheless, social media plays an increasing role in both terrorism and counterterrorism. Social media in fact pioneers development as it uses sophisticated artificial intelligence, algorithms and machine learning mainly for marketing and profit-making purposes. The Internet and specifically social media are the catalysts of terrorist recruitment and simple avenues to spread extremist ideologies. At its genesis, the Internet and social media may have been considered as utopian virtual mediums of free speech, sharing uncensored opinions through a network connecting people. The Internet was supposed to make people more tolerant, strengthen solidarity and encourage the equal and rapid distribution of reliable information. Unfortunately, this idealist and naive concept of the Internet is long defeated.

Social media today much rather isolates, creates alternative truths and polarizes thinking. Most platforms of social media such as YouTube, Twitter, Facebook, or Instagram, monitor and scan eagerly upon which content like buttons are pressed, which words and people are being searched for. Then, based on the analyses of its delicate algorithms the platform feeds new content selected to fit the behavior of the user. With its instant upload, share and download options, once a content uploaded to social media it is almost impossible to delete it completely and the number of its viewing increases exponentially. While the lack of regulation and censorship was once a great achievement of the Internet and social media, it now generates extremism and misinformation. This opportunity has not bypassed the attention of ISIS either. ISIS was very active on social media platforms, considering them the fuel to spread hatred and aggressive ideologies. This tactic helped ISIS carry out attacks even in Europe by remotely organizing and developing its terrorist network with lone or loosely connected sympathizers. This strategy helped ISIS recruit volunteers for terrorist attacks or fighters for its warfare in the Middle East.[33]

As such, social media basically poses two main concerns regarding terrorism: *(i)* first, it isolates users and pushes them more and more extreme content, and *(ii)* second, it provides for a more effective intimidation and message delivery on a global scale. The first concern is the result of the profit and market orientated

33 *Cf.* Imran Awan, 'Cyber-Extremism: Isis and the Power of Social Media', *Society*, Vol. 54, Issue 2, 2017, pp. 138-149.

operation of tech companies such as Facebook or YouTube. They spy on their users to make them addicted to the platform with content and more importantly advertisements which pleases them. As they purposefully deprive users from alternative or opposing opinions, they enclose them in a mental quarantine and possibly increasingly extreme ideologies. The second threat stems from the global nature of the network, where terrorists can easily reach 'target markets' in all parts of the world spreading violent and bloody images for intimidation. In both cases – *i.e*. extremization and intimidation – terrorists use social media platforms for communication, to deliver special messages. In the first case, they use it for recruiting new members for the cause. The recipients are potential terrorists, the result is when they join. In the second case, social media platforms are used to spread fear and to shock. The recipients are ordinary people, the desired result is intimidation.

Naturally, some sort of regulation and censorship became inevitable. Partly the presence and success of ISIS on social media, partly the political debates on sexism, racism and fake news in the US led to the monitoring and filtering of content on almost all social media platforms. The filtering and takedown of posts may be done in two ways. These are either based on notifications of the users or they may be completely automatic. In the first case, users make a notification in case a content is problematic, and the operator of the platform may delete the post. This system typically requires human control as it yields less content to monitor. *Nota bene*, it is also possible that due to the sheer number of notifications, the site automatically deletes content following a certain number of notifications. Another way is the application of algorithms which filter and monitor all posts published on the website. Algorithms therefore filter notions and expressions which *usually* encourage aggression and violence. Obviously, this system is not without problems. It may lead to taking down harmless, humorous or educative content, whereas it may be unable to detect dangerous content where the latter uses indirect or coded phrasing. The fight against terrorism almost always results in some restriction on the liberty of citizens. This, however, does not mean that algorithms should be neglected in counterterrorism.

Algorithms may be used for counterterrorism with more promising results once they are equipped with machine learning (ML). ML is a form of Artificial Intelligence (AI). AI has the capacity of a computer, robot or software which enables human-like cognitive functioning.[34] The biggest breakthrough of AI as of yet is its ability to learn. Therefore, relying on database input, the machine is capable recognizing and identifying an object, a picture or sound in real life or in the digital sphere. Following an adequate learning and cognitive process, AI can also perform analogue 'thinking'. Hence, based on its earlier knowledge and decisions, it may be able to recognize and categorize items which were not programmed in its memory.[35]

34 *Cf*. B. J. Copeland, 'Artificial intelligence', *Encyclopedia Britannica*, at www.britannica.com/technology/artificial-intelligence.

35 Enrique Lee Huamaní *et al*., 'Machine Learning Techniques to Visualize and Predict Terrorist Attacks Worldwide using the Global Terrorism Database', *International Journal of Advanced Computer Science and Applications*, Vol. 11, Issue 4, 2020, p. 563.

AI is therefore a non-organic, manmade intelligence capable of analyzing, identifying or categorizing, with the ability of making decisions accordingly. For instance, a self-driving car stops when it detects a stop sign.

ML may operate purely in the digital world when analyzing data and making decisions with algorithms. The foundation of all ML is one or more databases. ML analyses the data and makes a prognosis on the result of the process, hence, it arrives at conclusions with relatively great precision and accuracy.

ML can be used for counterterrorism as well. On the one hand, it processes and filters posts published on social media platforms through grammatical analysis or the image and sound content of videos uploaded to YouTube. Then it may label some of them as dangerous or offensive and it may either notify the user or take down the content automatically. ML may also be applied to make predictions to flag potential terrorist risks in different regions or countries so that decision-makers may prepare for threats.[36] One research in this field created an ML attached to the Global Terrorism Database which collects data of terrorist attacks starting with 1970.[37] The algorithm could predict where and with what probability a terrorist attack may take place, but evidently it could not detect future perpetrators or exact location and time.[38] Currently, ML is not advanced enough to provide adequate predictions for prevention and there are also some concerns when it comes to identifying and classifying terrorist content. The problem lies in its inaccuracy. The greater the database used by ML, the greater the chance for misidentification.[39]

It is evident that state interference in the freedom of the Internet is necessary to protect citizens against terrorism, extremism, and violence in general. Yet one cannot deny that it results in the limitation of liberty. It also means that the state may use ML and social media as an infrastructure for collecting information about its citizens. In fact, it is quite tempting for a state to abuse this power.

Social Media and ML may disrupt public trust, social integrity, the concepts of reality and valid information. Moreover, they disrupt legal concepts as well, as it is not clear who is the responsible for conducting related cyber-actions. The state, the owner and operator of the platform or solely the user? What happens if the actual user and content creator is not discernible? Which factor determines which state has jurisdiction to investigate and prosecute the case?

As far as the state's abuse of social media and ML is concerned, human rights and data protection law may provide some answers, but their substance and enforcement differ from state to state. International law may only contribute to this field through the protection of human rights, yet, on a global scale, it seems too general, and on the regional level, it is highly fragmented as well.

36 James T. Bang *et al*., *Predicting Terrorism: A Machine Learning Approach*, 2017, at www.researchgate.net/publication/321341137_Predicting_Terrorism_A_Machine_Learning_Approach.

37 Huamaní *et al*. 2020, p. 562.

38 H. M. Verhelst *et al*., 'Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security', *Science and Engineering Ethics*, Vol. 26, Issue 6, 2020, p. 2977.

39 Id. p. 2969.

doi: 10.5553/HYIEL/266627012023011001017

2.1.4. Investigation and Surveillance with Big Data

Counterterrorism and national security services for their part actively use advanced technology for detecting criminal plans, preventing attacks and for arresting or eliminating perpetrators. In fact, often those terrorists who are planning or carrying out attacks are already under observation and tracked by the competent authorities.

Big Data is similar to social media in the sense that it is also a network of shared information. Big Data, however, does not connect persons like social media. It links databases creating a vast network of data. Big Data is data management on a massive scale, which collects, stores, connects, uses and analyses a huge amount and variety of dynamic (*i.e.* constantly changing) data from several sources.[40] Big Data may be used for commercial or financial purposes to analyze markets and the behavior of users. But Big Data also provides opportunities in the investigation stage of counterterrorism and crime prevention.

Big Data is an excellent tool for surveillance since it is a massive network of information covering almost all aspects of life from professional to personal, just like the telescreen in Orwell's classic, *1984*. This dataset allows the state deploy maintain intelligence services and surveillance against potential terrorists and criminals at a hitherto inconceivable scale. In this interconnected and data based world, almost all movements and actions of persons can be recorded as data. Most of these data are stored in online databases and cloud networks. The Internet (the link between the networks, hence the name) provides access and transition between these data sources – and Big Data uses this interconnected global network. This way, Big Data combines and compares variable dynamic data from different sources and links these data with the help of algorithms. With such a pool of information, analyses and conclusions can be made to a depth and accuracy never seen before. Moreover, Big Data uses ML to achieve even better results. Algorithms process an ever-growing quantity of data, which allows them to gain even more 'experience', rendering them capable of performing advanced cognitive functions. This means that state counterterrorism offices may form a Big Data network and cover almost all aspects of the suspect's life. It is well-known that a similar system operates in China, unfortunately, for a different purpose, illustrating that everyone can be monitored.

The above sheds light on another important characteristic of Big Data: it is not designed to monitor only a limited number of suspects. Nor is it possible to do so. For adequate efficiency it is not enough to process the data only attributable to the suspect. Indeed, it inevitably implies collecting, managing and processing the data of other persons as well. A vast data bank is vital to prevent crimes, to obtain evidence or to initiate an investigation against a person yet unknown. It is crucial to have all the relevant data related to all potential offenders (that is, everyone). This includes recording phone conversations, saving private emails and chats, storing credit card information, money transfers, monitoring social media activity, travel data, saving street surveillance records or browsing history. The main point

40 Tom Breur, 'Statistical Power Analysis and the contemporary "crisis" in social sciences', *Journal of Marketing Analytics*, Vol. 4, Issue 2-3, 2016, pp. 61-65.

here is that today almost of the above listed data are stored online or in the cloud. Therefore, most if not all of these datasets are directly or indirectly connected. Those who can access, connect and process all these data in a comprehensive and holistic way may be able to identify the perpetrators of a terrorist attack, may be able to catch and arrest them, and may be able to prove them guilty before the courts. In time, should ML advance even more, there may also be a real chance for preventing these atrocities from happening. The cost of this effective way of policing is of course the loss of our right to privacy: losing a significant aspect of our freedom and bearing the worrying risk that the state may abuse its power. Big Data may be turned against the state's own citizens. In China, Big Data, surveillance and the extensive application of IT cause tensions with human rights organizations and some democratic states, as the communist regime intends to use this vast database and center of analysis to control its citizens by applying a score system.[41] This Orwellian method is surely suitable for spreading fear among the civilian population, in the knowledge that enemies of the regime are often punished with death or in other violent ways.

2.2. Cybercrimes in a Digital Era

All of the above-mentioned technologies are segments of a new reality, that is, the digital reality. AM prints based on digital CAD files (blueprint), drones are either controlled digitally or are completely autonomous, whereas social media, ML and Big Data are in the front line of actually shaping this new virtual reality. However, we do not need to go so far: almost every aspect of our modern life depends on the digital world. Just to give some quite evident examples: government services and registers are available online, postal services track deliveries digitally and online, all financial data are stored online, energy plants, dams, nuclear reactors use digital systems and store relevant data online. All infrastructural services are controlled digitally, including our water supply, electricity and heating. Most business transactions are tracked and executed online and digitally. Cyberspace is a massive, inconceivable domain which completely overlaps with our physical reality. Basically, besides and alongside our real, biological and physical world, there is another one, built on data and mathematics. It is both fascinating and worrying at the same time.

Since every institution and infrastructure is present and dependent on the digital sphere, those who can access and modify it, have the potential to destroy, or at least disrupt these systems and therefore the lives of millions. This means that hackers may break into well-protected and sophisticated public or private digital systems. They have the potential to paralyze data traffic and wreak havoc by entering and disrupting air or railway traffic control. A talented hacker can cause chaos in financial registers, commercial flows or energy supply should they be able to gain control of the relevant systems. It is possible to break down national election systems, alter results, or simply render them invalid. In essence, hackers exhibit an increasing potential to control a huge portion of social functioning. They can cause panic, rebellion and even death. In short, it appears that new technologies

41 *See* at www.chinafile.com/conversation/Is-Big-Data-Increasing-Beijing-Capacity-Control%3F.

doi: 10.5553/HYIEL/266627012023011001017

have the potential to become a more effective, even global way of committing terrorist attacks.

2.3. Rule of Law as the Best Defence System

The above mentioned forms of advanced technology, share a significant trait: they are disruptive to the shared values, the security and the safety of peoples. This essay argues, that in this sense, the described examples of disruptive technology can be considered as new forms of terrorism since their aim is to break down the unity and order of society by spreading fear amongst the civilian population. Whether carried out by individuals, criminal groups or by the state itself, these forms of terrorism must be addressed by national law and international law, which must afford proper protection against violence and fear. The way any law can ensure both the protection of public order and the respect of freedoms is through the rule of law, be it on the national or international level.

3. The Role of International Rule of Law in Tackling the Dangers of Disruptive Technology

The executive has the power and the infrastructure to use massive technology and professional staff to guarantee order. Order *per se* is not a question of law, it is a question of having the necessary tools and power to achieve it. Yet, one cannot overlook the fact that quite frankly, this very ability of the state executive poses a huge threat in itself, as well. Where there are no limits to the function of the state in upholding social order, this can easily lead to autocracy. In autocracies, there is order, and quite a solid one, however it is neither a safe, nor a liberal order. According to the theory of social contract, we expect the state to ensure a just and secure order, which by its very nature guarantees our freedoms. More precisely, we need protection against the disruptive use of technology both by non-state actors and states, so that our freedom and security are respected equally. This is where the law comes in. Individuals and the state are both bound by law, as such, law ensures security and accountability, in short, a just order. This secure and just order is the core of society. Humanity created societies of different structures with the same goal: to achieve security and welfare for individuals and the group as a whole, to collectively protect themselves against violence, such as terrorism.[42] And the rule of law is the most useful guarantee to that end.[43]

Rule of law is conceivable both in the terrain of domestic and international law. Rule of law faces two different challenges on these two levels. On the domestic level, rule of law must mitigate the risks posed by a strong, centralized power, whereas on the international arena, it is expected to respond to the reality created

42 *I.e.* all violent or disruptive actions – either by individuals or the State – against the order, integrity and values of the community by endangering their (sense of) security.

43 Hisashi Owada, 'International Terrorism and the Rule of Law', *Swiss Review of International and European Law*, Vol. 20, Issue 4, 2010, p. 503.

doi: 10.5553/HYIEL/266627012023011001017

by equal sovereigns without a centralized authority.[44] The way one looks at the international rule of law, however, may be influenced hugely by an ethnocentric perspective. While a common law jurist sees the rule of law as a set of individual and procedural rights against political power, continental lawyers follow the *Rechtstaat* approach instead, where state powers are limited by the means of public law and public institutions.[45] This difference resembles the way international law itself may be understood. The public law approach considers international law an institutionalized and constitutionalized legal order.[46] By contrast, others believe that international law is the counterpart of domestic private law, as it operates between equal and independent entities, the states.[47] This later theory points to one significant element of public international law. The sovereign equality of states means they can shape their legal obligations and can conclude and withdraw from treaties, they can amend or make reservations to international agreements. Hence, they may construct most of their legal obligations.[48] This reveals a harsh reality. International rule of law "is not a synonym for general justice, still less for democratic values."[49] Nevertheless, rule of law has always had one common objective on both the domestic and international level. Rule of law means the principle of legality[50] under which law constrains arbitrary exercise of power so that both the subjects and the creators of the law are bound by the rules.[51] Moreover, the ancient principle of *non sub homine sed sub Deo et lege*[52] suggests that rule of law has some material requirements for being not only legal, that is objective and predictable, but also just. Accordingly, rule of law is a complex legal and moral reality which obliges both the individuals and the states at the national and international level.

Although the focus of this study is on the international legal framework, evidently, international law may only serve as a residual or last resort solution. As it is stated, the most effective tool is the executive at the domestic level, and the international cooperation of the national systems. However, there must be a legal ground for the monitoring, the prevention, the investigation, and the prosecution activity of such institutions. Naturally, legal obligations must bind all of these activities and the internal rule of law should prevail, either by the common law

44 Ian Hurd, 'The International Rule of Law and the Domestic Analogy', *Global Constitutionalism*, Vol. 4, Issue 3, 2015, p. 366.

45 Miodrag A. Jovanovic, 'Responsibility to Protect and the International Rule of Law', *Chinese Journal of International Law*, Vol. 14, Issue 4, 2015, p. 768.

46 Clemens A. Feinaugle, 'The UN Declaration on the Rule of Law and the Application of the Rule of Law to the UN: A Reconstruction from an International Public Authority Perspective', *Goettingen Journal of International Law*, Vol. 7, Issue 1, 2016, p. 160.

47 Sir Hersch Lauterpacht, *The Function of Law in the International Community*, Oxford University Press, Oxford, 2011, p. 432.

48 Hurd 2015, p. 379.

49 James Crawford, 'International Law and the Rule of Law', *Adelaide Law Review*, Vol. 24, Issue 1, 2003, p. 4.

50 Jovanovic 2015, p. 768.

51 Crawford 2013, p. 10.

52 "Not under men but under God and the law." *Cf.* Rupa Bhattacharyya, 'Establishing a Rule-of-Law International Criminal Justice System', *Texas International Law Journal*, Vol. 31, Issue 1, 1996, p. 62.

doi: 10.5553/HYIEL/266627012023011001017

approach – through providing individual substantial and procedural rights, or by the continental approach – by establishing watchdog institutions. Then, provided that there are legal grounds for it, national courts my proceed. The domestic system, however, might be ineffective, being subjective or oppressed, when the atrocities are carried out by the state, the state representatives or entities under the protection of the state. In this case, international law may play a role, but it is not necessarily the first option. Regional mechanisms seem to be more effective, more accepted and they certainly have a more significant role in influencing national practice. Therefore, their practices implemented by regional and national systems may contribute to the international regime.[53]

However, history tells us that it can work the other way round just as well. Often, the only possibility to step up against oppressing and bloody regimes – either by establishing individual or the state responsibility – was to enforce the norms of public international law. Indeed, prosecuting individuals is most effective on the domestic level. Except, when the individuals or the groups are affiliated with the state. Disruptive technology will most probably be abused by states, or actors affiliated with the states. Simply by the fact that they have access to the data sources, the infrastructure and the professional staff. They have the most reasons to do so as well: to control their fellow citizens. Regional solutions might not be fully effective, mainly, because in most cases, they are not designed to enforce universal values. Public international law, however, has always played a strong role in ensuring or at least emphasizing these imperatives.

The point is, national law and domestic rule of law may only be effective until the state in question respects and maintains it. This level may provide the most effective protection against disruptive technology should it be abused by non-state actors. Once it is the state who misuses technology against other states or its citizens – in breach of domestic rule of law – only regional or international legal solutions can help.

International law has limited possibilities to enforce its norms. Should the abuse of advanced technology be committed by individuals and reach a certain level of atrocity, international criminal law may be applied before the International Criminal Court (ICC), or another specifically established *ad hoc* or hybrid international court. Should the actions be attributable to the state, State Responsibility (SR) may be invoked, even before the ICJ. The ICC is a last resort solution, it being a complementary court. It may only be a practical choice if the national system is too corrupt or too broken to serve justice. SR may be invoked in any case where the state breaches humanitarian law, treaty law, human rights or customary norms of international law. It is to be noted, however, that a procedure before the ICJ is unlikely in case of disruptive technology use. Therefore, disruptive technology may challenge the contemporary concepts on intervention, since intervention seems to be the only plausible and realistic – even if not necessarily lawful – tool for enforcing the imperative norms of international law.

53 Following Amnon Reichman's critical thoughts expressed during The 4th Young Researchers Workshop on Terrorism and Belligerency, 11 October 2021. The event was recorded and made available online at www.youtube.com/watch?v=q-8uVZDYciQ.

3.1. Attack by Disruptive Technology – Is It Terrorism?

This study does not cover domestic or regional aspects of criminal law, instead, it raises the question whether disruptive technology may be tantamount to terrorism. It may seem bizarre at first sight to claim that the use of disruptive technology against the population is tantamount to terrorism. However, it fits rather perfectly to the concept and definition of terrorism accepted by the international community.

Although there is no general definition of terrorism *per se*, which is exemplified by the fact that the UN itself rather regulates and defines some typical forms of terrorism separately, without treating terrorism as a general concept.[54] Nevertheless, the International Convention for the Suppression of the Financing of Terrorism provides an overall definition which serves as a supplementary *actus reus* added to the other forms of terrorism determined by international treaties.[55] The definition stipulates that besides the specified acts in the treaties against terrorism, terrorism is:

> "Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."[56]

Considering the fact that the Convention currently has 189 state parties,[57] it is safe to assume that since the vast majority of the international community has accepted the definition, it can at least serve as a reference for determining international terrorism.

The abuse of disruptive technology can meet the criteria set out in this definition. These actions are intentionally carried out against the civilian population, they either endanger the lives or the safety of citizens or actually cause death and/or injury. The aim is often to intimidate the population or to compel the government in some ways. Although it is an expansive interpretation, I believe

54 Javier Ruperez, 'The United Nations in The Fight Against Terrorism', *132nd International Senior Seminar, Visiting Experts Papers*, 2005, p. 14, at www.unafei.or.jp/publications/pdf/RS_No71/No71_07VE_Ruperez.pdf.

55 *Cf. inter alia*: 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft; 1970 Convention for the Suppression of Unlawful Seizure of Aircraft; 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; 1979 International Convention against the Taking of Hostages; 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation; 1997 International Convention for the Suppression of Terrorist Bombings; 2005 International Convention for the Suppression of Acts of Nuclear Terrorism; 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation; 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft; 2014 Protocol to the Convention on Offences and Certain other Acts Committed on Board Aircraft.

56 International Convention for the Suppression of the Financing of Terrorism, 1999, Article 1(1)(b).

57 *See* at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-11&chapter=18&clang=_en.

doi: 10.5553/HYIEL/266627012023011001017

that the last part – compel the government – should be interpreted to include destabilize or break the conventional – democratic – institutional framework of a certain state. And it can even be carried out by the state – meaning that the state or certain branches of state power may use technology to dismantle individual and collective freedoms, accountability, legal guarantees and thereby forcibly change the political, economic, cultural and legal system of the state – hence, transforming the country into an autocracy. In that case, evidently, domestic legal institutions, watchdog units and the civil society are silenced and intimidated. It can be regarded as terrorism, as it uses the same tools: attacking the civilian population and it results in the same intimidation and/or enforced change of the political structure.

3.2. State Abuse of Disruptive Technology as State Terror? May Intervention Be the Solution?

Assuming that states are likely to use technology to monitor, control, limit and even persecute their citizens, can they be considered terror states? Should these practices be regarded as state terrorism?

Autocratic states can be quite innovative when they have a temptation to oppress, intimidate or torture their subjects. The way the Nazi state apparatus used the modern means of telecommunication, propaganda and industrialized infrastructure to kill millions of Jews, or the way the Hutu leaders used media (mainly radio and television) to incite an unimaginable hatred against the Tutsi minority are early examples that states can and are willing to use latest technology for heinous goals. The nuclear tests carried out in North-Korea worry the international community immensely as it is not certain that the regime would not use it in aggressive ways to intimidate its opponents with nuclear terrorism.

It is needless to say that the state is the most potent actor on the international arena to develop and use synthetically created or modified viruses or to develop new weapons of mass destruction with the newly created synthetical materials manufactured by AM. Therefore, the international community must be prepared to be able to react in a timely and effective manner to such dangers. International law typically defines terrorism as committed by individuals or non-state actors. However, at least empirically, can this doctrine be challenged?

Ironically, terrorism and terror itself was first attributed to states. The notion first appeared to describe the violent actions of the Jacobin state during the French revolution after declaring the Terror as a response to threats of foreign invasion.[58] Later, the term terrorist was identified with nihilist, anarchist, leftist or nationalist assassins, describing as such actions against the state.[59] Terrorism has become an everyday part of the public discussion following the attacks against the World Trade Center and the Pentagon. From then on, terrorism was largely attached to non-state groups.[60] It is clear, that the term has a complex history which has

58 Gilbert Guillaume, 'Terrorism and International Law', *International and Comparative Law Quarterly*, Vol. 53, Issue 3, 2004, pp. 537-538.

59 Id. p. 538.

60 Rumyana Grozdanova, '"Terrorism" – Too Elusive a Term for an International Legal Definition?', *Netherlands International Law Review*, Vol. 61, Issue 3, 2014, p. 323.

covered state aggression, individual assassinations and international actions of non-state formations. Clearly, in lack of a proper legal definition, empirically, terrorism may be the act of a state or individuals.[61] Consequently, being a heavily debated notion, terrorism may have different meanings in law, politics, sociology, or the public opinion.[62] The problem is that in practice, it is the states – both at the international and the domestic level – who decide who or what is to be considered as terrorist, hence, it remains their sovereign discretion to define the meaning of terrorism.[63] Nevertheless, there is still a consensus – not necessarily a legal one – on the actual substance of terrorism. Therefore, terrorism may be any abhorrent act of violence against a civilian population[64] which instils extreme fear from an indirect, relatively unknown threat[65] violating and endangering fundamental human rights and democratic values.[66] This definition-like description of terrorism resembles the ruling of the Special Tribunal for Lebanon (STL), the first tribunal at the international level to have jurisdiction over acts of terrorism.[67] It held that the crime of terrorism has three constitutive elements: *(i)* a volitional commission of an act, *(ii)* which creates public danger, *(iii)* with the intent of the perpetrator to cause a state of terror.[68] Although the existence of the international crime of terrorism in customary international law was heavily contested,[69] and the STL was a criminal court, and therefore only made this definition in connection to individual perpetrators, jurisprudence is familiar with the concept of state terrorism. State terrorism has two meanings: first, the systematic use of violence against the civilian population for the purpose of intimidation, and second, the same actions described by the international conventions on terrorism if supported by states.[70] Therefore, state terrorism is usually equated with dictatorships and autocratic regimes.[71] Indeed, it is widely known that terrorism is a dangerous tool which has

61 Rosalyn Higgins, 'The General International Law of Terrorism', in Maurice Flory & Rosalyn Higgins (eds.), *International Law and Terrorism*, Routledge, London, 1997, p. 28.

62 Alex Schmid, "Terrorism – The Definitional Problem', *Case Western Reserve Journal of International Law*, Vol. 36, Issue 2, 2004, p. 395.

63 Grozdanova 2014, pp. 318-319.

64 Sundaresh Menon, 'International Terrorism and Human Rights', *Asian Journal of International Law*, Vol. 4, Issue 1, 2014, p. 3.

65 Guillaume 2004, p. 537.

66 A/RES/60/288, Resolution adopted by the General Assembly on 8 September 2006.

67 Elies van Sliedregt & Larissa van den Herik, 'Introduction: The STL Interlocutory Decision on the Definition of Terrorism – Judicial Ingenuity or Radicalism?', *Leiden Journal of International Law*, Vol. 24, Issue 3, 2011, p. 651.

68 UN Special Tribunal for Lebanon (Appeals Chamber), Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, STL-11-01/I, 16 February 2011, para. 147.

69 Van Sliedregt & van den Herik 2011, p. 654.

70 Daniel O'Donnell, 'International treaties against terrorism and the use of terrorism during armed conflict and by armed forces', *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 875.

71 Emilio Crenzel, 'Inside 'State Terrorism': Bureaucracies and Social Attitudes in Response to Enforced Disappearance of Persons in Argentina', *Journal of Human Rights Practice*, Vol. 10, Issue 2, 2018, p. 271.

doi: 10.5553/HYIEL/266627012023011001017

often been used by states to obtain their desired political goals.[72] Repressive regimes therefore resort to aggressive intimidation to destroy the opposition party or the critical media,[73] and in general, to uphold their autocratic regime. This is becoming easier with the help of technology and surveillance. Nevertheless, is it possible to hold the state responsible for actions which empirically fit the criteria of terrorism?

Despite the fact that according to international law states may be considered as actors executing terrorist actions,[74] the distinction between individuals and the states usually means that individuals commit the terrorist attack, whereas the state may only be responsible for an omission.[75] The reason is that international terrorism suppression conventions oblige the states to prevent and to criminalize the acts of terrorism, to prosecute the perpetrators and to accept universal jurisdiction over crimes falling under the scope of the treaties concerned.[76] Therefore, the highest involvement of a state in a terrorist attack – as per the contemporary legal framework – may be the support of terrorist activity.[77] Such involvement is usually denied by the states.[78] For this reason, it is hardly well-established from a legal point of view, that states can actually and actively perpetrate terrorism. Consequently, should a state act resemble terrorism, the legal grounds for state responsibility would most probably be different, but certainly not terrorism itself, as the Teheran hostage situation has clearly showed.[79] A state may be held responsible for breaching international humanitarian law and specifically articles of the Geneva Conventions expressly prohibiting acts of terror.[80] Alternatively, actions resembling international terrorism carried out by states may also be seen as an act of aggression.[81] The problem is that international humanitarian law only applies in a situation of armed conflict be it international or domestic; therefore, the majority and the most classic forms of state terrorism cannot be assessed on the basis of humanitarian law norms. State responsibility may be an asset in holding a state responsible for the internationally wrongful act of aggression following an international mission using force against or in the territory of another state, but internal terror, carried out by autocratic states cannot be considered aggression. One solution may be the extensive interpretation of the international terrorism suppression conventions. Kimberley N. Trapp suggests for instance using the *Bosnia Genocide case* as an analogy.[82] Accordingly, as

72 Kimberley N. Trapp, 'Holding States Responsible for Terrorism before the International Court of Justice', *Journal of International Dispute Settlement*, Vol. 3, Issue 2, 2012, p. 283.
73 *Cf*. O'Donnell 2006, p. 870.
74 Trapp 2012, p. 283.
75 Guillaume 2004, p. 544.
76 O'Donnell 2006, p. 856.
77 Guillaume 2004, p. 544.
78 Trapp 2012, pp. 279-80.
79 Id. p. 295.
80 *Cf*. Article 33 of the Fourth Geneva Convention 1949; Article 51(2) of Protocol I on international armed conflict; 13(2) of Protocol II on non-international armed conflict; Article 4(2) of Additional Protocol II. For more detail, *see* O'Donnell 2006, p. 863.
81 Article 2(4) UN Charter; *see* Definition of Aggression, UN General Assembly Resolution 3314(XXIX).
82 Trapp 2012, pp. 281-282.

the prohibition of state genocide can be derived from the obligation of the states to prevent genocide, the same logic could be used regarding terrorism.[83] This might be a challenge before the judicial panel of the ICJ, but states themselves seem reluctant to accept the notion of state terrorism. A comprehensive and general draft convention on terrorism does not include the prohibition of state terrorism, although some suggestions were made to this effect.[84] Moreover, the draft explicitly rules out its application when the offences are committed within a single state.[85] Therefore, the draft follows the already existing approach, namely, that international law only applies to the international dimension of terrorism.

Yet, what justifies this surrender of the international legal order? International law regulates acts of terror performed by state actors during an armed conflict by the Geneva Conventions. International use of force by states resembling terrorism is considered to be aggression or interference in internal affairs, yet, if any act with similar characteristics but within a single state occurs, the international community and international law retreats immediately? Of course, *jus cogens* norms and human rights are applicable, but the way these norms may be enforced seems rather weak. The problem is evidently the fact that states may determine their own political, economic, social and cultural systems.[86] No other state[87] or the UN may interfere with this sovereign right, except, temporarily, the UN Security Council under Chapter VII.[88] This procedure, however, is only applicable when international peace and security is in danger.[89] Moreover, the Security Council operates on a political basis and indeed it is a political organ of the UN, therefore it is quite unlikely that it would step up against autocratic regimes because of their oppressing nature *per se*. The truth is that when state terrorism happens only on a domestic level, meaning that the state maintains a state of terror, violating fundamental human rights and spreading fear, it leads in *in praxi* to the lack of the rule of law in its domestic meaning. The reason why international law does not regulate internal terrorist acts of a state *per se* is because internal terrorism can be labelled most simply as autocracy. These practices of dictatorships are the opposite of a democratic society where the concept of the rule of law governs social interaction and the exercise of power. In a dictatorship law is the subjective and *ad hoc* order of power without normative limits. This is why international law cannot regulate this phenomenon. Because it is the fundamental structure, hence the political, social, cultural and economic system of the state – *i.e.* the internal affair of the state. Consequently, state terrorism as a system, the state of terror cannot be assessed by the international community with legal tools. At a maximum, it may discern some

83 Id.
84 Report of the Ad Hoc Committee for 2005, A/59/37, Annex I, para. 15.
85 Report of the coordinator on the results of the informal consultations on a draft comprehensive convention on international terrorism held from 25 to 29 July 2005, A/59/894, Appendix II, Article 3.
86 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, 1970 A/RES/25/2625.
87 Id.
88 Article 2(7) UN Charter.
89 Id. Article 52.

doi: 10.5553/HYIEL/266627012023011001017

aspects of this exercise of power such as human rights violations or breaches of relating international agreements. More precisely, the international rule of law – international legality – cannot enforce the internal rule of law within a state.

For this reason, it is very hard to imagine that international law may impose its legal – and moral – preferences on these states. Examples show that the heavily debated institution of (humanitarian) intervention is the only tool which may not be legal but seems to be (in some cases) effective.

Most of the brutal terror states were overthrown by collective or individual intervention of other states. Nazi Germany was eliminated by the Allies – although this was not intervention *stricto sensu*, but a classic war. The bloodshed of the Bangladesh Liberation War was terminated by the Indian military actions in 1971.[90] The genocidal realm of the Khmer Rouge and the heinous dictator, Pol Pot was swept out from Cambodia by the Vietnamese intervention forces in 1978.[91] In Kosovo, the NATO forces could prevent ethnic cleansing and the unfolding humanitarian catastrophe in 1999.[92] In Haiti, "the violent and unconstitutional actions of the Haitian military forces were immediately and strongly condemned by the international community.[93] The US intervened and a more democratic regime could develop.[94] In 2000, the British military intervention could halt violence and helped reach relative stability in Sierra Leone.[95] A good example for a more favorable collective intervention was in Darfur where the civil war reached the point of war crimes, crimes against humanity and even genocide. The joint mission of the UN and the forces of the African Union aimed to mitigate the brutality.[96]

There is a huge debate about the legality of interventions. It is also true that their success is often highly questionable, sometimes they are a complete failure. Yet, it seems that intervention really is the *ultima ratio* of the international legal regime to enforce its norms. Today, individual intervention without the authorization of the UN is unlawful. However, the abuse of disruptive technology may be defeated by using technology in cyberspace too. And this could challenge the conventional idea of state sovereignty and the role of international law. As such, it may disrupt the notion of intervention, leading towards a new concept of cyber-intervention.[97] Intervention requires moral and legal grounds: this legal ground can be the failure of the state to protect its citizens against terror, violence and oppression.

90 Navine Murshid, 'India's Role in Bangladesh's War of Independence: Humanitarianism or Self-Interest?', *Economic and Political Weekly*, Vol. 46, Issue 52, 2011, pp. 53-60.

91 *See* at www.britannica.com/place/Cambodia/Vietnamese-intervention.

92 *See* at www.nato.int/cps/en/natolive/topics_48818.htm.

93 *See* at https://peacekeeping.un.org/sites/default/files/past/unmihbackgr2.html.

94 Judson Jefferies, 'The United States and Haiti: An Exercise in Intervention', *Caribbean Quarterly*, Vol. 47, Issue 4, 2001, pp. 71-94.

95 *See* at https://researchcentre.army.gov.au/library/occasional-papers/rapid-intervention-and-conflict-resolution-british-military-intervention-sierra-leone-2000-2002.

96 UN Security Council Resolution 1769, adopted on 31 July 2007.

97 Following Amnon Reichman's suggestions during The 4th Young Researchers Workshop on Terrorism and Belligerency, 11 October 2021.

3.2.1. The Responsibility of the State to Protect its Population against Terrorism

The expectation for protecting the fundamental human rights and the safety of the civilian population is not a new phenomenon in public international law. The international community has always had the temptation to step up against the most heinous atrocities committed by individuals or states. In the past these were rather unsophisticated and counterproductive measures such as humanitarian intervention.[98] Owing to the often abusive application of already existing forms of intervention, the International Commission on Intervention and State Sovereignty proposed a concept under the name of Responsibility to Protect.[99] Protecting the population of a given state against violent atrocities has become an international effort.[100] The UN acknowledged the report in its 2005 World Summit Outcome[101] and the Secretary General has contributed towards developing and elaborating the principle of R2P with annual reports afterwards. The R2P regime rests on a three-pillar system.[102] The first pillar is the responsibility of the state to protect its population, as the main addressees of this obligation have always been the states.[103] This protection requires the state to refrain from actions which may lead to atrocity crimes, and it also obliges to states to prevent such actions by active capacity building.[104] The second pillar concerns the international community in helping this capacity building which includes the cooperation of states, international organizations, civil society organizations as well as the UN itself.[105] The third pillar demands a timely and decisive response from the international community should a state cannot or did not want to fulfil its obligation to protect.[106] It allows the possibility, moreover imposes the obligation for intervention. The problem is that R2P enlists only four crimes from which the state shall protect its population. These are genocide, war crimes, crimes against humanity and ethnic cleansing.[107] Clearly, terrorism or the abuse of disruptive technology is not included. Unless of course the atrocities also fulfil the criteria of crimes against humanity which is quite likely. That way the R2P can also cover disruptive technology from which the civilian population shall be protected under its regime.

One may argue that already existing norms such as antiterrorist agreements, human rights, or the Wassenaar Arrangement[108] also oblige the states to prevent terrorism in their territory by capacity building, education, criminalizing and

98 Gábor Sulyok, 'The Legality of Humanitarian Intervention under Traditional International Law', *Acta Juridica Hungarica*, Vol. 46, Issue 3-4, 2005, p. 224.

99 ICISS Report 2001, Ottawa, para. 1.40, p. 9.

100 ICISS Report 2001, Ottawa, para. 2.4, p. 11.

101 A/60/L.1 2005, World Summit Outcome, Articles 138-140.

102 A/63/677 (2009), Implementing the responsibility to protect: Report of the Secretary General, p. 2.

103 A/69/981-S/2015/500 (2015), A vital and enduring commitment: implementing the responsibility to protect: Report of the Secretary General, para. 7, p. 17.

104 A/63/677 (2009), para. 11(a), pp. 8-9.

105 Id. para. 11(b), p. 9.

106 Id. para. 11(c), p. 9.

107 A/60/L.1 2005 World Summit Outcome, Article 138.

108 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, especially its 2013 Amendment restricting technology used for surveillance and extract data.

doi: 10.5553/HYIEL/266627012023011001017

prosecuting terrorism as well as enhancing international police cooperation. Although it is unquestionable that these rules of public international law do oblige the state for such actions, but this fragmented regulation cannot provide such an overall and holistic regime as R2P. Yet, it seems unlikely as of today that the malicious misuse of technology by states could be accepted as a ground for a military intervention. And the other problem is that the contemporary legal framework does not accept the existence of state terrorism, therefore it rather concentrates on how the state may constrain non-state actors and individuals from committing terror crimes. However, the development in technology may force changes in this respect as a few states are more than willing to use the advanced technology to intimidate or to attack their own civilian population. But it may also mean, that the international community or states may use technology for intervention – based either on UN authorization or the notion of self-defence.

3.2.2. Cyber-Intervention against Disruptive Technology

Cyber-intervention basically means that one or more states intervene in the national cyberspace of another state by technological means. National cyberspace is, however, a fluid notion.

> "A nation's cyberspace is part of what can be regarded as the global cyberspace as it cannot be isolated in order to chalk out or define its boundaries since the concept itself is boundless, contrary to the physical world-land, seas, rivers and air that is regulated by geographically demarcated boundaries."[109]

There is a wide consensus among states that such intervention is against the principle of non-intervention. In more evident cases, where there is an eminent result in the real world, the breach of non-intervention is clear:

> "An act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, may constitute an unlawful intervention, depending on the circumstances, and at any rate, it may constitute a violation of sovereignty."[110]

Some states, like France consider cyberthreat so dangerous, that they are prepared to the take *ultima ratio* steps, should the interference reach a critical point. As France declared:

> "Depending on the extent of their intrusion or their effects, they may violate the principles of sovereignty, non-intervention or even the prohibition of the threat or use of force. States targeted by such cyberattacks are entitled to respond to them within the framework of the options offered by international

109 Abhilash Pattnaik & Soumya Kumar Palo, 'Cyber Sovereignty: A Dichotomy', *The GNLU Law Review*, Vol. 5, p. 71.

110 *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, Ministry of Foreign Affairs of Japan, 28 May 2021, p. 3, at www.mofa.go.jp/files/100200935.pdf.

> law. In response to a cyberattack, France may consider diplomatic responses to certain incidents, countermeasures, or even coercive action by the armed forces if an attack constitutes armed aggression."[111]

The possible responses my vary, but the consensus is clear, cyber-intervention is the breach of the principle of non-intervention.[112]

However, two points must be made here. *(i)* First, these state declarations are made in connection with cyberspace attacks, *i.e.* against the abusive use of technology. It is evident that these cyber-interventions are unlawful. Nevertheless, this paper tries answer to the question, whether protective cyber-intervention as a sanction could be applied against the state who carries out, support or tolerates the abusive use of disruptive technology either against other states or against its own people. *(ii)* Therefore, the second point is that the above declarations do not cover the potential use of cyber-intervention as a tool to enforce international norms against oppressive and violent states.

Two cases must be examined here. The first case is when a state or its population is targeted by disrupted technology and the attack comes from another state – directly or by supporting, tolerating the actions of individuals. The second scenario is when the state uses technology against its own population to maintain a state of terror and the international community or another state provides help to the civilian population by enforcing the norms of international law. In both cases two issues should be considered. How can we classify the empirically understood cyber-intervention? Does the cyber-action violate the sovereignty of the state?

In the first scenario, it is evident that the state against which the cyber-intervention is employed is the victim of an internationally wrongful act of another state. It may also be true if the attack is not directly carried out by the state, but by private actors in its territory, instead. Should such state not follow the *aut dedere aut judicare* principle, or even facilitate and support the commission of the attack, the act is attributable to it, since the

111 *International Law Applied to Operations in Cyberspace*, Ministry of Defense of France, 9 September 2019, at www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

112 *Cf.* US: Hon. Paul C. Ney, Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 March, 2020; UK: United Kingdom Foreign, Commonwealth & Development Office, Application of international law to states' conduct in cyberspace: UK statement, 3 June 2021; Germany: Federal Government of Germany, On the Application of International Law in Cyberspace, March 2021, pp. 4-6; Iran: Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, August 2020; Italy: Italian position paper on "International law and cyberspace", Italian Ministry for Foreign Affairs and International Cooperation, pp. 4-5; The Netherlands: Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace, 26 September 2019, p. 3; New-Zealand: The Application of International Law to State Activity in Cyberspace, 1 December 2020, p. 2; Switzerland: Federal Department of Foreign Affairs, Switzerland's position paper on the application of international law in cyberspace, May 2021, p. 3.

doi: 10.5553/HYIEL/266627012023011001017

> "State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[113]

Therefore, it must tolerate the 'hack backs' of the injured state.[114] Especially, if the internationally wrongful act is directly attributable to the state. *Prima facie*, this action of the attacked state may look like intervention, however, dogmatically it rather fits the definition of countermeasure. This is because they are the response of the injured state, which action would have been unlawful without the wrongful act of the attacking state.[115] These are therefore the self-help tools of injured states.[116] This also applies to the cyber context.[117] It is worth mentioning that should the cyberattack reach the level of the use of force, the potential digital response of the victimized state would rather be an action of self-defence. Otherwise, it is more likely that cyber-intervention would not reach the force threshold, and the response would only be a countermeasure in cyberspace.[118] Needless to say that under this scenario, the cyber-response would not be qualified as intervention, and qualifying as self-defence or countermeasure instead, it will not breach the sovereignty of the targeted state who has abused its sovereign powers first.

The second scenario is more complex as it addresses the old dilemma with a new twist. The already known aspect is whether the international community or a state individually has the right to intervene should a state establish and maintain an autocratic, oppressive and intimidating regime internally. The fact that this terror state would be maintained by the abuse of technology does not change the nature of the question. However, there is a novelty, if one considers the possibility of a purely digital or cyber intervention. Imagine a violent, aggressive autocracy which intimidates and persecutes its population by using the latest technology. It may use massive surveillance, drones, Big Data and ML to filter critical elements of society and it may use synthetic biology or AM technology to create and stock a new weapon arsenal as a threat. Evidently, the power of such state would be dependent on technology. A technology which would inevitably be digital, therefore cyber and interconnected. This digital dependence may be turned against that state. If one, that is the state or the international community could hack the system, it could paralyze the entire system. It may freeze financial systems or traffic which would be essential for the functioning of the apparatus, it may shut down the laboratories and factories where AM and synthetic biology produce and

113 Michael N. Schmitt (ed.), *Tallinn Manual On The International Law Applicable To Cyber Warfare*, Cambridge University Press, Cambridge, 2013, p. 26 (Rule 5).

114 Michael N. Schmitt & Sean Watts, 'Collective Cyber Countermeasures?', *Harvard National Security Journal*, Vol. 12, Issue 2, 2021, p. 374.

115 'Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries' *Yearbook of the International Law Commission*, Vol. II, Part Two, 2001, Part Three, Chapter II(1).

116 Id. (2).

117 Schmitt 2021, p. 398.

118 William Banks, 'Cyber Attribution and State Responsibility', *International Law Studies Series*, Vol. 97, 2021, p. 1064.

store the weapons. It might paralyze or even delete data used and analysed by surveillance and employing elements of Big Data for the purposes of intimidation. Essentially, a digital autocracy may be defeated solely in cyberspace. The old question is whether (cyber)intervention may be lawful – yet disruptive technology poses a challenge in answering this question. Cyber-intervention may not even be intervention. This paper argues that such cyber-actions would rather fall under the notion of sanctions.

Sanctions differ from countermeasures as they are not the reactions of the injured party, but are rather imposed by the creator of the breached norm. In the case of international law, they are imposed by the international community. The application of sanctions, *vis-à-vis* intervention, clearly shows that the domain falls under the regime of international law. Sovereignty is far from being boundless. It is now understood that some matters, such as human rights or *jus cogens* norms impose limitations under international law.[119] Accordingly,

> "[…]' justifications for sovereignty no longer rest exclusively on sovereignty's own presumptive legitimacy, but rather expand to incorporate justifications that derive from the individuals whose rights are to be protected, and from their right to a safe framework in which they can enforce their autonomy and pursue their interests."[120]

The international community may enforce these criteria by implementing sanctions. Already existing sanctions include freezing of bank accounts, travel bans, weapon or commercial embargoes, no-fly zones, *etc*. Their essential purpose is to break the wrongdoer by trying to paralyze its systems. Cyber-intervention is just like that, the only difference being that it may be much more effective and much easier to implement. In that way, the correct term referring to such actions would be cyber-sanctions. And it is not only a dogmatic issue when it comes to terminology. Intervention has a strong negative connotation and has always been associated with misuse and self-interest – it has always been an abusive, aggressive terminology. Sanctions on the other hand can be attributed to law enforcement instead, i.e. as just and effective consequences applied against the wrongdoer.

4. Summary

Disruptive technology has the potential to significantly raise the threat of terror, abuse of human rights and democratic values. The new digital era may challenge our sentiment of security, our certainty in facts and our trust in social institutions. But technology can also provide answers to protect our values and the most important norms of humanity. Contemporary domestic legal systems and international law seems to provide answers on a normative level to protect people

119 Michael N. Schmitt, 'Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention', *International Law Studies Series*, Vol. 96, 2020, p. 559.

120 Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', *Cornell International Law Journal*, Vol. 48, Issue 3, 2015, p. 492.

doi: 10.5553/HYIEL/266627012023011001017

against the abuse of disruptive technology. AM and new, possible weapons of mass destruction, drone attacks, synthetic biology and ABC weapons, social media, ML or Big Data do not challenge significantly the normative aspects of the legal systems. However, they do challenge the enforcement of these already existing norms. It is also worrying that technology is most likely to be misused by the state against another state or against its own population. This opportunity may be seized by autocratic states, who may monitor, control and determine almost all segments of human lives. This paper has argued that the abuse of disruptive technology may be tantamount to terrorism and terror states in their methodology and their effect.

The most promising way to protect the population against both threats is to strengthen the concept of the rule of law, both in its domestic and international sense. Rule of law is a complex legal and moral reality which helps maintain both order and liberty. The protection of its citizens is the duty of the state and, indeed the domestic level is the most effective and practical domain to counter the dangers of disruptive technology. The domestic system, however, is paralyzed when the abuser is the state itself. In such cases, international law may provide *ultima ratio* solutions. State Responsibility may be invoked against states who breach their international obligations. Yet, since the abuse of technology may be best described as autocracy, traditional forms of state responsibility may not be effective. Disruptive technology, challenges the notion of intervention when carried out in cyberspace. Following a cyber-attack, injured states may 'hack back' as a form of self-defence or, rather, as a digital countermeasure. Cyber-sanctions may be imposed by the international community against a terror state to paralyze its systems and to enforce the peremptory norms of international law. In both cases, the risky terminology of intervention should be avoided, using the less debated notions of countermeasure and sanctions.