ICT for peace foundation

POLICY
PAPER

# FROM BOOTS ON THE GROUND TO BYTES IN CYBERSPACE:

## A Mapping Study on the Use of Information CommunicationsTechnologies (ICTs) in Security Services provided by Commercial Actors

Anne-Marie Buzatu

**GENEVA 2022**
ICT4Peace Foundation

The author would like to thank the Swiss Federal Department of Foreign Affair's Peace and Security Division for their generous support in funding this mapping study. The author is also grateful for the excellent and substantive contributions to the mapping study by the following people: Sanija Ameti, Jelena Aparac, Maria Cattaui, Martin Dahinden, Adriana Alvarez Enrique, Michael Møller, Daniel Stauffacher and Mauro Vignati, as well as to the more than 40 people who participated in interviews and workshops in order to bring the policy paper to life.

ICT4Peace Publishing, Geneva, September 2022
Copies available from www.ict4peace.org

# CONTENTS

# CONTENTS

# FOREWORD

ICT4Peace is proud to have been mandated by the Swiss Foreign Ministry to carry out this timely and urgently needed mapping Study on the emerging use of ICTs in private security services by commercial actors. The increasing proliferation of new commercial actors using ICTs bring additional human rights concerns to the ones already existing in the industry of traditional physical security companies. This study is providing, for the first time, a comprehensive mapping of these companies and its categories, description of risks to human rights emanating from this emerging sector and highlights potential gaps in governance and regulatory frameworks, that the international community needs to address.

As the study makes clear, this emerging economic sector poses considerable conceptual and definitional challenges, since we are leaving the world of traditional private security companies that typically perform tasks that traditionally belong to the state's monopoly on the use of force through military and police. We are entering the cyber realm, where private sector actors can be equally important players as Governments. This state of affairs provide additional, political and regulatory challenges to Governments and private actors alike. But it’s another prime example of the need of the international community to become aware of these new risks and to adapt our governance frameworks as technology evolves.

There is no person better equipped than Anne-Marie Buzatu, Vice-President and COO of ICT4Peace, to lead this important work. For over ten years Anne-Marie Buzatu has played an important role in improving oversight and accountability of the private security industry, making important contributions to the development of the Montreux Document on Private Military and Security Companies, and leading the development of the International Code of Conduct for Private Security Service Providers (ICoC) and its oversight mechanism. As more and more of our lives shift online, bringing along new and surprising challenges to governance and human rights, this study marks the first step in taking stock of the accompanying human security risks, and provides guidance on the next steps to tackling these important, evolving challenges.

Daniel Stauffacher
Founder and President
ICT4Peace Foundation

# EXECUTIVE SUMMARY

This Mapping Study aims to shed light on how commercial actors are using information and communications technologies (ICTs) in the provision of private security services. The original idea behind the study was to look at how "traditional, boots on the ground" private security companies, such as the members of the International Code of Conduct Association (ICoCA), were incorporating ICTs into physical security offerings. However, research and interviews painted a more complex portrait of how ICTs were being used by commercial actors in security-related activities and services, including anti-terrorism, intelligence-gathering, digital forensics and protection against cyberattacks.

Importantly, the findings highlight that the capture, storage, analysis and utilization of a multitude of data points or information is intrinsically intertwined with security services and security provision, and that this information acquisition and instrumentalisation in the information age in which we live impacts our enjoyment of human rights. Therefore, a human-centric approach to private security services requires practices that safeguard information.

Looking through a human-security lens, the study takes stock of the evolving nature of the private security sector, identifying characteristics of commercially provided ICT-enabled security services that are similar as well as different to earlier private security paradigms. In particular it highlights four important shifts in the contextual underpinnings of the notion of "security":

1) State-centric to human-centric,
2) State actor to private actor,
3) Territorial to extraterritorial, and most recently
4) Physical to virtual.

In so doing, it explains some of the characteristics particular to ICTs, and highlights human rights risks and security impacts posed by these services.

It then takes stock of other relevant oversight and governance initiatives that have endeavored to fill some governance gaps posed by commercial actors impacting human rights, providing a recent historical overview with a view to identifying lessons learned and good practices that could be applied to the use of ICTs in private security services.

The heart of the study, the actual mapping of the kinds and types of uses of ICTs in the provision of security services, follows. In presenting the different kinds of ICT-enabled private security services, several case studies are included in order to help bring them to life and to illustrate more vividly the human rights impacts and risks. A special section is devoted to the use of ICTs in the conflict in Ukraine, which began during the latter stages of research for this study.

This is followed by a consideration of human rights impacts and cross-cutting issues as well as the translation of principles such as due diligence, transparency and accountability into the ICT space.

The study finishes with some recommendations for next steps:

- Identify gaps in existing relevant norms and regulatory frameworks;
- Update existing relevant regulatory frameworks;
- Coordinate it through a multistakeholder platform;
- Develop effective oversight and remedial processes;
- Develop capacity-building for relevant companies.

# LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| - | AI | Artificial Intelligence |
| - | CBMs | Confidence Building Measures |
| - | CCTV | Closed Circuit Television |
| - | CII | Critical Infrastructure Installation |
| - | COCOM | The Coordinating Committee for Multilateral Export Controls |
| - | COMINT | Electronic Communications Intelligence |
| - | CSO | Civil Society Organisations |
| - | FOC | Freedom Online Coalition |
| - | GFCE | Global Forum Cyber Expertise |
| - | GGE | Group of Governmental Experts |
| - | GNI | Global Network Initiative |
| - | ICoC | International Code of Conduct for Private Security Companies |
| - | ICoCA | International Code of Conduct Association |
| - | ICRC | International Committee of the Red Cross |
| - | ICS | Industrial Control Systems |
| - | ICTs | Information and Communications Technologies |
| - | IGF | Internet Governance Forum |
| - | IRA | Internet Research Agency |
| - | LAWS | Lethal Autonomous Weapons Systems |
| - | MSTC | Microsoft Threat Intelligence Center |
| - | NSA | US National Security Agency |
| - | OEWG | Open-Ended Working Group |
| - | OSINT | Open Source Intelligence |
| - | POA | Programme of Action |
| - | POW | Prisoner of War |
| - | PMSCs | Private Military and Security Companies |
| - | PSCs | Private Security Companies |
| - | RFID | Radio Frequency Identification |
| - | SCADA | Supervisory Control and Data Acquisition |
| - | SIGINT | Signals Intelligence |
| - | SORM | Russian System for Operative Investigative Activities |
| - | UAV | Unarmed Arial Vehicles |
| - | UN | United Nations |
| - | UNGPs | The UN Guiding Principles on Business and Human Rights |
| - | VPI | Voluntary Principles Initiative |
| - | VPSHR | Voluntary Principles on Security and Human Rights |

## Mapping Study on the use of ICTs in private security services by commercial actors

### Introduction

How are new technologies impacting the private security sector? Information and communications technologies (ICTs)[1] are evolving at exponentially increasing rates, with new developments arriving continuously. These developments are impacting and transforming nearly all facets of modern society, including the private sector, which is continuously incorporating new technologies into its security service offerings, as well as offering new kinds of security services.

However, how these technologically-driven offerings are impacting and altering the private security sector is less well understood. The sheer number of technology advances that are being developed by primarily private actors, as well as the speed at which they are continually being integrated into private security service offerings, introduces new considerations, elements to contend with as well as important but often unrecognized concerns for human rights protections. As we increasingly rely on ICTs to express opinions, interact with others, carry out financial transactions, perform work functions or even just have fun, the information and data that is collected by these technological means can be used to invade our private lives, and to commit other serious violations of our human rights.

Furthermore, the increasing proliferation of commercial actors using ICTs to provide a wide array of security services introduces new kinds of actors outside of the “traditional” private security company, bringing additional human rights concerns to those that were originally considered in PMSC regulatory frameworks, including the Montreux Document and the International Code of Conduct for Private Security Service Providers (ICoC). More and more companies are being created around the world to offer these kinds of services, as demonstrated by quantitative research.[2] Additionally, the dizzying-pace at which technology is evolving as well as its exponentially increasing complexity poses significant challenges to effective governance and oversight: terms such as “cybersecurity” and “cyberattack” do not have standardized definitions, and the term “private security services” as defined in the ICoC is outdated and does not correspond to the current reality of private security service provision.

[1] For the purposes of this paper, ICTs are defined as a diverse set of technological tools and resources used to capture, transmit, store, create, secure, damage, delete, share, analyze or exchange information. These technological tools and resources include but are not limited to their use in computers, the Internet and internet connected devices, software and apps used for intelligence gathering and analyzing, risk reduction/prevention and other security purposes, devices to capture biometrics, video surveillance, robotics, drones and telephony (fixed or mobile, satellite, GPS).

[2] See Annex II.

Finally, the way in which ICTs are changing private security services is often little or poorly understood, with increasing “weaponization” of information, “smart” products taking decisions instead of humans and dual-use technologies blurring well established lines between benign and more malevolent activities. This results in many concerning practices and consequences for the rule of law and for the protection of human rights.

In response to these important challenges, this mapping study aims to shed light on the current “state of play” of ICTs in private security service provision through a human rights lens. In presenting this mapping, the paper groups activities into several overarching categories, identifies the kinds of technologies that are used, the actors that are providing them, and the uses these services are put to. Potential human rights risks will be identified, as well as weaknesses and gaps in existing regulatory frameworks. In so doing, it also looks to other multistakeholder and business and human rights initiatives which have dealt with similar and related issues, and which could provide concrete guidance. It is hoped that this approach will help to provide greater clarity on how ICTs are shaping and changing private security services, identify potential human rights risks as well as to provide ideas for more effective oversight and governance of these services.

The paper has five main parts: a conceptual section which presents the main challenges posed by the use of ICTS in providing private security services, a section which chronicles the development of other relevant governance initiatives, the main section in which these services are identified, categorized and explained, a fourth section which considers cross-cutting issues and good practices and lessons learned that could be applied to this sector, and a final section which takes stock, looks forward and considers what further work is required to improve governance and oversight of these services. The war in Ukraine began when we were in the latter stages of the development of this paper, and is still ongoing at the time of writing, however we have endeavored to include some relevant examples of ICTs used in the conflict in this paper, with a view to going into more depth in follow-up research at a later date.

In preparing this paper, the author carried out a review of the relevant literature, researched the services provided by International Code of Conduct Association for Private Security Service Providers (ICoCA) member companies and followed up with requests to some companies for interviews, and organized two workshops with ICoCA members from both companies and civil society. Additional interviews were held with experts from private security companies, governments, members of civil society, academic and other subject matter-experts.[3]

[3] For a list of the experts, see Annex I.

## The evolving nature of the Private Security Sector

Private security services are not a new phenomenon and have been growing steadily since the end of the Cold War, as state armed forces have been downsized, and the need for specialized security services has been on the rise.[4] However, this shift from public to private security provision has brought along its own governance challenges. With physical private security teams, often composed of persons of multiple nationalities frequently traveling across increasingly porous borders, even functional national oversight regimes find it difficult to hold persons no longer on their territory accountable. Alongside the evolution of the private security sector is the evolution of the notion of security itself, with a marked shift from it being associated with the security of the state to also including security of the individual, or "human security."[5] Post 9-11, the "security response to the nature of global threats" has been increasingly framed as a" function of new technologies" with greater reliance on surveillance and data mining technologies[6]. The massive on-boarding of securitized ICTs further challenges governance frameworks as they allow for accumulating huge amounts of personal data and information, as well as "action at a distance", or a physical separation between the one using or controlling the ICTs and their resulting impacts, which may be felt in different jurisdictions.

### *Setting the stage*

"The nature of the private security sector is characterized by two elements: the provision of security services, and their delivery by non-state actors." This statement, which kicked off a 2015 policy paper on regulation of "traditional" private security companies[7] holds true several years later, even with the increasing use of ICTs in provision of security services. However, some of the assumptions and understandings have shifted. In 2015, the understanding of "private military and security services" was very much those provided by "guys with guns," or physical protection of persons and places. The "non-state actors" delivering those services were the physical persons carrying those guns, often wearing military-style clothing that nevertheless was not provided by the state. Together, these elements painted a picture of danger and potential violence; they elicited images of "enhanced interrogations," shooting massacres, mercenaries. Contrast this with an image of a not very physically imposing guy whose main light exposure may be the glow from his computer screen.

The dissonance between those two images helps to illustrate why it is conceptually challenging to include the use of ICTs as part of private security services: one depicts an imminent threat; the other doesn't look threatening at all. Until recently, the human rights aspects of ICTs used in private security services was at most an afterthought. However, as

[4] Buzatu, Anne-Marie, *Towards an International Code of Conduct for Private Security Providers: A View from Inside a Multistakeholder Process*, DCAF SSR Paper 12 (2015), p.10 [last accessed 7 July 2022].

[5] See below the Box on "The Evolution of 'Security'".

[6] Vincenzo Pavone, David-Olivier Jaquet-Cchiffelle "A systemic approach to security: Beyond the trade-off between security and liberty, *Academia,* 2016 last accessed 22 May 2022

[7]See, e.g., Buzatu, DCAF SSR Paper 12.

ICTs have infiltrated nearly every aspect of people's daily lives in the developed world, with more people from emerging and developing nations coming online every day, their misuse can violate human rights on a much larger scale. Examples include creating a chilling effect on the freedom of expression and association, forcibly returning refugees to countries where they face threats of torture or death, or even delivering attacks that physically injure/ cause death. In order to respond to these human rights risks, the challenges posed by private security services need an update and reboot.

*Scope and considerations*

This paper aims to carry out a mapping of security services using ICTs provided by the commercial sector. Initially, it was envisaged as carrying out an examination of how "traditional, boots on the ground" "private security companies" (PSCs) or "private military and security companies" (PMSCs)[8] are incorporating ICTs in their private service offerings. However, through research and interviews it soon became clear that such definitions and scope would not contain an accurate "current state of play" of how ICTs are impacting and shaping security services provided by commercial actors. Certainly, research indicates that P(M)SCs are incorporating ICTs in nearly every aspect of their service offerings. However, a significant portion of these companies have also ventured into purely "cybersecurity"[9] service offerings with no obvious physical/armed component. In addition to cybersecurity services, products and services of so-called "cyber mercenaries" deploying cyber surveillance capabilities to governments using them to oppress critical journalists and human rights defenders also feature prominently in reports about ICTs used ostensibly for security purposes. It has become clear that mapping the ways in which ICTs are being commercially deployed towards so-called security ends with impacts on human rights requires a larger field of action.

*The evolution of "security"*

At its core, security can be described as protection from harm or freedom from fear, however the underlying assumptions of, and responses to ensuring security have shifted over the centuries. These underlying assumptions can be characterized along the shifts from:

1) state-centric to human-centric,
2) state actor to private actor,
3) territorial to extraterritorial, and most recently
4) physical to virtual.

Since the mid-seventeenth century, which was characterized by the **"law of coexistence"** where each state was responsible for security on its own territory, to the post WWII era of **"law of cooperation"** which saw a proliferation of international organi-

[8] as defined in the ICoC and Montreux Document respectively
[9] See section for definitions

zations working on areas of common human interest such as food security, public health and labour rights[10], to the post-Cold War recognition of **"human security"**[11] as an important organizing principle in multilateral fora, the notion of security has evolved in significant and substantial ways. With the advent of the Information Age, the meaning of security and the means to provide it have shifted again, with **security of information** taking on increasing importance. As one expert put it, "information is the new gold—maybe even more valuable." As our societies increasingly rely on ICTs to carry out a wide variety of activities, secure information, even support armed attacks, human-rights based standards for the uses it is put to, or **"digital human security"**[12], is becoming a prerequisite for free, secure and well-functioning democracies.

*What's in a name: mercenaries, PMSCs and PSCs*

As the state has progressively lost its monopoly on the use of the force, private actors for hire have increasingly stepped in, being referred to by different labels that were very much the product of their time and cultural context. As a point of departure, the term "mercenary" has been often seen within a negative light as persons primarily motivated by money rather than national allegiance and seen as a betrayal of sorts of the underlying assumption that the state should have the monopoly of force. With the downsizing of state military forces after the end of the Cold War, there was a growing recognition of a legitimate need for private actors to fill in some of the resulting gaps in the provision of military and security services, in particular to provide services that support international humanitarian law and human rights legal frameworks. This led to international initiatives identifying more clearly what the roles, responsibilities and limits of these actors were, giving rise to terms such as "private military and security companies" (PMSC) and "private security companies" (PSC).[13] Within the context of the Information Age, we see even more non-traditional actors providing security services utilizing ICTs, many of whom would never describe themselves as private security companies[14], raising the question of whether this calls for a new term. As will be discussed more below, South Africa is using the term "cybersecurity service provider", or CSSP to describe "the new private security industry". With this in mind, the terms "mercenaries", "private military and security companies" (PMSC) and "private security companies"(PSC) will be considered with a view to transposing them to the context of security services using ICTs.

Mercenaries

[10] See Buzatu, DCAF SSR Paper 12, at pp. 13-14.

[11] In its Human Development Report 1994, UNDP introduced the concept of "human security" which "equates security with people rather than territories, with development rather than arms.".

[12] See, e.g., Weekes, Barbara, "Digital Human Security 2020, Human security in the age of AI: Securing and empowering individuals" (2019) [Last accessed 7 July 2022]

[13] Switerland has been very much at the forefront of these efforts, leading initiatives including the Montreux Document and International Code of Conduct for Private Security Service Providers, which will be discussed in greater detail below.

[14] See e.g., the case studies below on Nokia's services in Russia and Microsoft's activities in Ukraine.

The Additional Protocol I to the 1949 Geneva Conventions was adopted in 1977 (API) and contained the first international definition of mercenaries. While it did not ban mercenarism as such, it did state that mercenaries didn't have the right to combatant or prisoner of war (POW) status. Furthermore, it detailed six cumulative conditions required for a person to be defined as a mercenary, all very much tied to fighting/directly participating in an armed conflict, but without a national or formal tie to a state party to the conflict, as well as participating with the motivation to do so "primarily by the desire for private gain."[15] The same definition of mercenaries was repeated within the 1977 Convention for the Elimination of Mercenarism in Africa (entry into force in 1985) and the 1989 International Convention against the Recruitment, Use, Financing and Training of Mercenaries (Mercenary Convention, entry into force in 2001), with both of these conventions taking the additional step of criminalizing mercenarism. As has been pointed out by numerous authors, the requirements of this approach are largely seen as unworkable, and to the author's knowledge the definition has never been successfully enforced either under API or the mercenary conventions.[16]

Private Military and Security Companies (PMSCs)

in the context of the armed conflicts of the mid-2000s, the Swiss government and the ICRC crafted a new term for the Montreux Document, "private miliary and security companies," which included a wider range of military and security activities that were provided within the context of an armed conflict, including "armed guarding and protection of persons and objects, such as convoys, buildings and other places, maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel." Of note, this definition doesn't make reference to fighting or directly participating in hostilities of an armed conflict, but it does primarily relate to those companies who are providing services within the context of an armed conflict.

Private Security Companies (PSCs)

[15] Article 47(2) of Additional Protocol defines a mercenary as any person who:
(a) is specially recruited locally or abroad in order to fight in an armed conflict;
(b) does, in fact, take a direct part in the hostilities;
(c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
(d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
(e) is not a member of the armed forces of a Party to the conflict; and
(f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

[16] Born and Buzatu, *Old Dog, New Trick: An overview of the contemporary regulation of private security and military contractors,* Sicherheit und Frieden (2008), p. 8. However, persons have been charged under national legislation, such as South Africa's Foreign Military Assistance Act for participating in military coups, although in many cases these charges were dropped. See, e.g., *Coup charge against 'mercenary' dropped*, last accessed 27 July 2022.

Taking a broader approach to cover security services provided both on the battlefield as well as in times of peace, but in areas of weakened governance, the International Code of Conduct for Private Security Service Providers (ICoC, 2010) took aim to reduce violations of human rights by private commercial actors. The ICoC included the definition of "security services" provided by private security companies (PSCs) that included "guarding and protection of persons and objects, such as convoys, facilities, designated sites or property or other places (whether armed or unarmed), or any other activity where Personnel of Companies are required to carry or operate a weapon in the performance of their duties." This definition was built on the assumption that the most likely way that human rights would be violated by commercial security actors would be through physical violence or coercion.

Private Military and Security Companies, version 2

In 2011, the UN Working Group on the use of Mercenaries (UNWG) proposed a draft convention on PMSCs in which they include references which could apply to instances of PMSCs using ICTs. It defined PMSCs as a "corporate entity which provides on a compensatory basis military and/or security services by physical persons and/or legal entities" and then goes on to define "military services" as "specialized services related to military actions" and included such services as intelligence, satellite surveillance, "any kind of knowledge transfer with military applications."[17] "Security services" include "any kind of knowledge transfer with security and policing applications," as well as "development and implementation of informational security measures and other related activities." While the draft convention remains very much a draft[18], its definitions recognize the importance of information analysis and transfer as a part of military and security activities, as well as their potentials to violate human rights. In order to ensure that our existing legal frameworks remain relevant and provide their intended protections of the human population, work is needed to translate them to be effective vis-à-vis ICTs enabled security services.

*ICTs as goods and services*

As the forgoing discussion demonstrates, the terms used to define mercenaries, PMSCs are defined by the kinds and characteristics of the services those actors/entities provide. In similar fashion, this mapping approaches the topic from the side of the security services themselves. In taking a closer look at how ICTs are used in these services, the nature of security services utilizing ICTs requires further clarification, as they do not fall squarely within traditional distinctions between goods and services. Traditional economic theory holds that "goods" are tangible objects or products that can be touched, are excludable[19], whose ownership can be transferred, and which can be stored for a later or repeated use, while

[17] United Nations General Assembly, *Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council*, 13 May 2011, A/HRC/WG.10/1/2 [last accessed 7 July 2022].

[18] The UN Draft Convention on PMSCs has not progressed beyond the discussion phase. However, in 2017 an Intergovernmental Working Group was created "to elaborate the content of an international regulatory framework, without prejudging the nature thereof, relating to the activities of private military and security companies." For more information, see https://www.ohchr.org/en/hr-bodies/hrc/pms-cs/igwg-index/3rd-session-igwg-military [last accessed 8 September 2022].

[19] An "excludable good" is one in which if it is held by one actor, then another actor doesn't have it.

"services" denotes an activity of performing work for others. Software used to provide security services has many of the characteristics of goods, as it can sold in distinct units, its ownership can be transferred, and it can be used multiple times; it also has characteristics of services, because its processes are intangible, it can perform work for others and it can use intelligence to make determinations, predictions and propose solutions: its coding captures human and machine intelligence in a format that has durability and repeatability, but not typically excludability[20]. Similarly, a tangible good that is "smart", or which is operated or controlled by software, can also be transferred and used multiple times, but it can also provide services, such as analyze information, provide advice and make predictions. Along more traditional lines, there are services providing support to the use of these ICTs, which may be provided by humans, as well as increasingly by machines. Accordingly, this paper considers both the security services used to deploy technologies, as well as the "security services" provided by sale of software and hardware together, sometimes replacing physical security personnel, that are provided by commercial actors.

This is similar to the approaches of both the Montreux Document and ICoC, which listed different kinds of security services, and then identified the relevant commercial actors as those that provided those services, "irrespective of how they describe themselves."[21] Following a similar logic, this paper looks at the kinds of ICT-related services and products offered by commercial actors which aim to respond to risks of attacks or other incidents related to (human) security, peace and stability ("security services"), whether through physical or virtual means. Furthermore, it considers these services through a human security lens, identifying where the services may impact human rights. This approach recognizes the reality that many companies that would not call themselves "private security companies" are nevertheless providing these kinds of services, *and* that these services are impacting many fundamental rights and freedoms on a large scale.

*Human rights impacts*

When considering the impacts of ICTs used in security services provided by companies, initially the human rights impacts may seem disconnected, or at most "action at a distance," compared to the harm that can be inflicted by guns or other physical violence. As one representative from the private security sector told me, "private security using computers for human rights violations, I just don't get it." However, as that and conversations with other subject-matter experts from civil society, government, academia and the private security sector progressed[22], the picture came more clearly into focus.

[20] Blockchain technologies aim to be an exception by offering excludability to digital assets.

[21] Montreux Document, p. 9. ICoC, defines "Private Security Companies" as any Company…whose business activities include the provision of Security Services on its own behalf, or on behalf of another, irrespective of how such Company describes itself. Recognizing that the human rights considerations could be the same, he ICoC definition also made room for companies who provided security services for its own operations.

[22] See Annex, list of interviewees.

Many stakeholders expressed an uneasiness with the large amount of data that was being generated and collected everyday about the most personal aspects of their lives, tracking their whereabouts, interactions with others, expressions of opinion, and their preferences. More concretely, several recounted instances of when this information was used to surveil and identify targets and persons of interest and resulted in serious human rights impacts including restrictions on travel, psycho-socio-economic costs and even arrest, bodily harm and death.

As one civil society representative said, "the mass collection and surveillance of information by governments can lead to 'fishing expeditions'[23] in order to identify persons that may be critical or otherwise antipathetic to governments, making them targets for further human rights abuses." At first blush this mass collection of information may not square with the ideas of what private security companies are doing, and some companies may not see themselves as contributing to this at all. However, consider the following examples brought up by different experts:

- Video surveillance services using cameras equipped with facial recognition, silhouette recognition, body heat mapping and vehicle recognition technologies[24];
- Drones used to monitor borders and water crossings for would-be migrants or mining installations for so-called "artisanal miners",
- Intelligence services for sale which amass large amounts of information from open-sources (e.g., from social media platforms and metadata from emails), using artificial intelligence to analyze for patterns and anomalies in order to make predictions about future behavior.

These services and many more are currently being offered by ICoCA member companies, often with little regulation or oversight. As one private security provider told me, the use of "advanced technologies such as facial recognition and heat detection … in video surveillance are dictated by a client's budget", not by considerations of their impacts on human rights. As will become increasingly clear in later sections, limits on the use of intrusive and weaponized technologies are often dictated by market forces rather than regulation. Every day new technology capabilities and offerings are being added to the marketplace with little consideration of how they will impact (human) security.

In this fast evolving, transnational marketplace, private companies are using ICTs to offer security services at a scale never seen before, raising the following considerations:

[23] A "fishing expedition" is an informal, pejorative term for a non-specific, large-scale search for information, especially incriminating information.

[24] The research has so far not found instances of ICoCA members using armed drones.

- Asymmetric nature of private security obligations

When considering security services by private commercial actors, one element to keep in mind is the inherently asymmetric nature of the security provider's obligations. Private security providers' obligations are owed *to their client*, and not to others in the general population with whom they may come into contact or who may be impacted when they are carrying out services such as surveillance, intelligence gathering or operating drones.[25] This contrasts with public security officers who are tasked with providing security as a public good and are not particularly beholden to protect the security of one specific actor over another one.

- Invasion of privacy

As mentioned above, the huge amounts of information shared on social media platforms, apps, through sending emails, messages and browsing websites are analyzed by sophisticated algorithms to create personal profiles of users, including consumer preferences, political opinions, sexual orientation/preferences, and travel habits to name a few. While used for marketing and advertising purposes, this personal information can also be obtained by governments and used to identify and target individuals, particularly by governments with autocratic tendencies.[26] Perhaps less obvious are data collections made by video surveillance, access control systems, GPS location information, including location data "leaked" by advertisements on smartphones and other apps. Most of these are hosted by commercial actors, who obtain our "consent" when we agree with their privacy policies and terms of service in order to use their products and services. While each of these data points may not seem to be an important invasion of privacy in and of itself, taken together with the availability of data analyzing software services, they can help to construct a quite detailed profile of our personal characteristics and preferences.

- Discrimination and inequality

Technology has often been described as neutral however this is not the case with algorithms, which have been developed and fed data by humans, typically for profit or for defence purposes. In the words of UN Special Rapporteur on racism, Tendayi Achiume, technology is "fundamentally shaped by the racial, ethnic, gender and other inequalities prevalent in society, and typically makes these inequalities worse."[27] The repercussions of technologically-driven discrimination and bias are felt in nearly every aspect of life, "from education and

[25] National and local laws would apply, but particularly in the case of ICTs where the service provider is more likely to be located outside the jurisdiction in which the impacts of the service are felt, this poses serious challenges to effective oversight and accountability. See below.

[26] This, unfortunately, is the majority of governments. The 2022 Freedom House report identified a decline in democracy for the 16th year in a row, and only 20% of countries world-wide obtained the designation of "Free Countries."

[27] Tendayi Achiume, UN Special Rapporteur on racisim in report on Emerging Digital Technologies and Racial Discrmination : https://www.ohchr.org/en/press-releases/2020/07/emerging-digital-technologies-entrench-racial-inequality-un-expert-warns

employment to healthcare and criminal justice."[28] Along similar lines Timnet Gebru, the former co-lead of Google's ethical artificial intelligence (AI) team lost her position after co-authoring an article that raised concerns around the use of large-language AI models without considering their inherent racial and gender biases in the development of AI, biases that could "entrench existing inequalities, rather than help solve them".[29] Her departure sparked outrage, with two other Google AI researchers resigning in protest, and thousands of Google employees signing a petition condemning Google's actions, raising concerns about whether companies such as Google could be trusted to develop this technology in a way that was beneficial to humanity, and not just to their profit margins. This incident has shed a spotlight on one of the major concerns of AI development, which relies in large part on information created and developed primarily by men, and according to Gebru and many other AI experts, can include discriminatory biases in its computations.

On the other hand, one area of technology, facial recognition, that has been repeatedly labeled as having lower levels of accuracy among women and those with darker skin tones has drastically improved in recent years. This is not to say that facial recognition technology is perfect in its identification, but rather goes to the fact that physical differences between members of different populations and genders are not the reason that accurate identifications fail; rather these tend to be due to aging or injury, or lack of adequate datasets. [30] More generally, this goes to the constant evolution in technology, and also shows how emotionally-charged findings of a decade ago can remain in current discourse despite technological improvements. Furthermore, it highlights how good technology is getting at recognizing us and recording our whereabouts, contributing to privacy concerns.

- Freedom of thought and opinion, freedom of expression.

In today's information society, many communications and information exchanges take place on different digital platforms, including social media platforms, apps and email and messaging platforms. With powerful data analytics and sentiment analysis capabilities available on the market that can flag and follow postings and other online interactions, this contributes to a "Big Brother" mass surveillance ecosystem, which can have a chilling effect on freedom of thought, opinion and expression, discouraging free discourse and expression online and offline. In addition to the "chilling effect", there can also be actual suppression of expression through the use of algorithms that can identify undesirable speech and block it, prohibiting it from being shared with its intended recipients, as well as flag the sender to watching authorities as having sent undesirable content. This may not only impact freedom of expression and freedom of opinion, but also rights such as those related to health and well-

[28] Ibid.

[29] Perrigo, Billy, *Why Timnit Gebru Isn't Waiting for Big Tech to Fix AI's Problems*, *Time Magazine*, 18 January 2022 [last accessed 7 July 2022].

[30] Baker, Steward, The Flawed Claims about Bias in Facial Recognition, Lawfare Institute, 2 February 2022 [last accessed 7 July 2022].

being as has been seen during the pandemic when important health information was not allowed to be shared.[31]

- Bodily harm

ICTs can directly lead to physical harm if they are used in weapons systems, such as armed drones, or to disrupt systems vital for our well-being, including health-care and other critical infrastructure installations. Less direct are the kinds of physical harm that result from being surveilled online and targeted. Examples of the latter include the use of ICTs to carry out extensive surveillance on those critical of governments with a view to silencing/eliminating them.

One example of this which has received much attention in the news, and was even the subject of a documentary, was the murder of Jamal Khashoggi, which was alleged to have happened on the 2nd of October 2018 in in the Saudi Arabian consulate in Istanbul, Turkey. Khashoggi was a journalist, columnist for The Washington Post and critic of the Saudi government. Citizenlab found that the smartphones of Khashoggi's inner circle of close friends and family members', some of which were also Saudi dissidents, were infected with the tech surveillance software Pegasus, developed and sold by Israeli company NSO to the Saudi government, among others. By monitoring Khashoggi's communications with others, they were able to read and access his messages, many of which were critical of the Saudi government and discussed efforts to counter Saudi disinformation online.

**Box: Spotlight on ICT Technologies:**

| Technology | Description |
|---|---|
| Biometrics | Facial recognition, fingerprints, iris scans, silhouette recognition, voice recognition, heart-rate sensors, behavioural biometrics (e.g., how walk, speak, type on keyboard). |
| Artificial Intelligence (AI) | Capability of computer system to mimic human cognitive functions including learning and problem-solving. |
| Machine Learning | Application of AI that enables a computer to learn "on its own" without direct coding or instruction using mathematical models of data. |
| Metadata | Information stored within files that contains information such as the name, approximate location, and time created of/by the author, as well as intended recipient (in case of email or message). Metadata is often not encrypted. |

[31] See, e.g., Ruan, Lotus, Knockel, Jeffrey and Crete-Nishihata, Masashi, *Censored Contagion, How Information on the Coronavirus is Managed on Chinese Social Media*, Citizenlab, 3 March 2020 [last accessed 7 July 2022].

| | |
|---|---|
| Data Analytics | Transforms raw data into knowledge that can find trends, answer questions, make predictions and drive informed decision-making. |
| Malware | Malware is software designed to gain unauthorized access, obtain user credentials damage, destroy information, remotely control processes, hold information for ransom, or otherwise interfere with the ICT system's security. |

*ICT Vulnerabilities*

ICT vulnerabilities go to the heart of many of the ICT security risks, and therefore can also have a major impact on human rights. ICT vulnerabilities are weaknesses in computer software and hardware security. Cyber attackers who discover them or buy them from vendors can use them to bypass the security systems of ICTs and access, obtain, remotely control and destroy information or hold it for ransom; malware relies heavily on these vulnerabilities for carrying out exploits. "Zero-day exploits" are a kind of malware which makes use of ICT vulnerabilities that have not yet been made public or discovered by ICT vendors and have not yet been secured or "patched." ICT vulnerabilities including zero-day exploits are sold on different markets known as black markets and gray markets. Black markets are underground marketplaces located on the Dark Web[32] which may transact in sales of vulnerabilities for criminal purposes. Gray markets involve selling vulnerabilities to government authorities who use them for espionage as well as to build cyber weapons.

Case Study: Government Stockpiling of Exploits

In the mid-1990's, concerned by the rise of the nascent World Wide Web and what it might mean for national security, the US Central Intelligence Agency created a special working group to assess how the agency could use the Internet for intelligence purposes. Soon, US government contractors were finding computer exploits, which could command six-figure and up commissions, sourcing them from hackers around the world. 9-11 brought a further sense of urgency to the use of cyber exploits as a part of defense. Other governments joined the fray, driving up prices of exploits and energizing the zero-day grey market ecosystem, which is thriving to the time of this writing. The major buyers in this marketplace are government law-enforcement agencies, however some are bought by commercial and other non-state actors.

In August 2016, a Twitter account @shadowbrokers claimed to have hacked the US National Security Agency's (NSA) stockpile of cyber exploits, and now were putting them on auction to the highest bidder. Writing in a broken English, the post included a link to 300 MB of files that included hacking tools with names such as Epicbanana, Egregiousblunder and Buzzdirection. On closer inspection, it became clear that this was not a hoax, and that @shadowbrokers had

[32] The Dark Web is a part of the Internet that requires special software, configurations and/or authorizations to access. It is not indexed and can host marketplaces for illegal and sensitive transaction.

obtained real cyber exploits used by the US National Security Agency, including attacks that could penetrate some of the most commonly used cybersecurity systems; "[t]hey were all a cyberterrorist would need to break into government agencies, labs and corporate networks all over the world."[33] However, the files were just a small sampling of the cyber exploits they had acquired, which an entity calling itself @shadowbrokers were now putting up for auction. Furthermore, they indicated that if the auction reached one million Bitcoin, they would release all of the NSA cyber exploits online. At the end of October 2016, the @shadowbrokers put out another tweet entitled "Trick or Treat" where they posted the web addresses of NSA decoy servers, providing a map of secret NSA hacking operations around the world, including in China, Egypt, Germany, India, Mexico, North Korea, Russia, Taiwan, Venezuela and the UK, and ended the post with a threat to disrupt the US 2016 Presidential Election including the hashtag #hackelection2016. Investigations later pointed to the files being taken from an NSA employee's home computer by Kaspersky security software. Kaspersky essentially confirmed this, but said it was just the cybersecurity software doing its job, identifying malicious code.[34]

This case study illustrates the incredible security risks posed by zero-day exploits, as well as an example of a cybersecurity company "inadvertently" obtaining them through their security products/services, with potentially devastating effects. Furthermore, as mentioned above, the sale of zero-day exploits is a growing industry, with little to no regulation, oversight or accountability.

### *Governance challenges of ICTs*

The above section identifies a number of challenges posed by commercial actors using ICTs to human security. Further undermining human rights protection are several important characteristics of ICTs that render its good governance/effective oversight and accountability more difficult.

#### Ubiquity and transborder nature

ICTs are seemingly everywhere and are usually not constrained by physical borders. While the transborder nature of ICTs is not unique as such, the volume and speed at which ICTs cross across borders and jurisdictions brings a level of complexity that has not been seen before, with actors collaborating on ICT activities often working in multiple jurisdictions. The networked nature of ICTs, particularly with those systems hosted in the "cloud", means that teams working together can do so from different locations. Furthermore, the Covid pandemic has increased the number of people working from different physical locations, as people have adjusted to having online meetings in order to reduce their physical exposure to others. Many

[33] Pelroth, Nicole, *This is How They Tell Me the World Ends, The Cyber-Weapons Arms Race*, Bloomsbury Publishing, Kindle Edition (2021), p. 321.
[34] Ibid at 328.

companies have implemented policies which allow people to work remotely so long as they can connect online with their coworkers.

Additionally, with the number of non-democratic states with dubious or poor human rights records on the increase, this in effect creates areas of "weakened governance" for human rights within cyberspace, raising concerns about how such governments will use ICTs in security services, and calling for a reinforcement of "human security" standards and protections.

Private sector ownership

Another element which is not unique in and of itself, but the scale of which poses unique challenges, is the extent of private sector ownership and control over ICTs. With estimates hovering at around 85% of private sector ownership of ICT infrastructure, as well as being a sector where development is largely driven by commercial actors, ICTs, and the systems and capabilities and virtual spaces they create, are essentially a private sector province. This does not mean that they cannot be regulated and overseen by government authorities, however the effectiveness of this public governance is undermined by the complexity and transborder nature described above. One way of looking at this is through the notion of "effective control" which underpins state sovereignty: in many of the constituent parts that make up cyberspace, technical (commercial) private sector actors are able to exert "effective control" where states are unable to, and the different systems and even the persons who control them may reside in different state jurisdictions, outside the "effective control" of any one state.

Lack of transparency and explainability

ICTs pose particular challenges to effective governance through their lack of transparency and explainability. This is particularly true in the case of AI and machine learning, in which results and predictions may be reached without humans understanding how. Also known as the "black box" problem, lack of transparency and explainability can also go to the identification of new problems and priorities that were not foreseen, nor are understood, by those who programmed or tasked them.[35] This can give rise to some situations that our current legal and governance frameworks are not equipped to manage. For example, who/what bears responsibility for harms caused by automated decisions where the systems' creators do not understand how they were reached or could have even reasonably foreseen such a situation? As former UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression David Kaye has warned, persons are unlikely to be aware of the "scope, extent and even existence of the algorithmic decision-making processes that may have an impact on

[35] Michael Pizzi, Mila Romanoff, Tim Englehardt, *AI for Humanitarian Action*, ICRC International Review: https://international-review.icrc.org/articles/ai-humanitarian-action-human-rights-ethics-913, p.9

their enjoyment of rights," and therefore effective notice about their use is "almost inherently unavailable."[36]

Lack of clear definitions and standards

"Cyber", "cybersecurity", "cyberweapon" and "cyberattack" and other similar terms are freely used in numerous venues by academics, government officials, security professionals, representatives of civil society, humanitarian organizations and international organizations, among others. However, without clear definitions for what these terms denote, a single term can be used to mean very different things. For example, while one actor may understand "cybersecurity" to mean the protection of computer hardware and systems, another actor may understand it to describe the field of peace and stability in cyberspace, including areas such as weaponization of information—two very different fields of application. This lack of precision in what these terms refer to and what they mean contribute to confusion and misunderstanding and more importantly make it difficult to understand exactly how they impact security and human rights.

Plethora of different initiatives

Further adding to the governance challenges of ICTs are the sheer number of ICT governance initiatives that have been launched, many overlapping or misaligned, some focusing on some very specific areas, making it difficult to keep up with all of the different initiatives. While this paper has mentioned some of the more prominent of these initiatives, these are just a small percentage of the total number of ICT governance initiatives, which for the most part have done little to effectively address human rights impacts of ICTs. This raises the question of how to approach the topic in a manner that can effect positive change with concrete results.

Lack of accountability and effective remedies

Taken together, all of these governance challenges make it difficult to put in place functional mechanisms that protect people from misuses and abuses of ICTs that negatively impact and violate human rights, as well as to provide effective remedies for human rights injuries. Cyberspace can be called an area of "weakened or fragile governance" requiring pragmatic approaches to protecting human rights, including important responsibilities on private actors.

**Regulating private commercial actors impacts on human rights: a recent historical overview**

While the above challenges are significant, they are not wholly without precedent. After the end of the Cold War, there was increasing recognition of the impacts of companies' activities on human rights, particularly in areas of weakened governance, and there were a number of initiatives that sought to mitigate these negative impacts.

[36] David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/73/348, 29 August 2018, para. 40, speaking about the application of AI in the online information environment.

*Relevant Oversight and Governance Initiatives*

There have been a number of initiatives launched to reduce/prevent negative human rights impacts on commercial actors. Many were launched in response to the increasing number of private sector security actors arising out of the end of the Cold War where state armies were downsized and they were hired to meet shortfalls. Others were launched to respond to the growing importance of ICTs' impacts on human rights. While certainly not exhaustive, below follows a list of initiatives developed to curb negative impacts on human rights by commercial actors and fill governance gaps, with a view to identifying and translating lessons learned to the use of ICTs in security services.

UN Convention on the use of Mercenaries (1989, entry into force 2001)

The UN Convention on the use of Mercenaries was finalized in 1989. The convention itself has been divisive along Global North/South lines, with most (but not all) signatories coming from less developed nations. Additionally, and as mentioned above, the Convention's definition of a mercenary is notoriously difficult to meet, with six cumulative conditions including finding that a person was largely motivated by financial gain to fight in a conflict / take part in hostilities. As such, the Convention has not been effective in curbing "mercenarism".

In July 2005, then United Nations Commission on Human Rights created a UN Working Group on the use of mercenaries. The Working Group is mandated to study and identify sources and causes, emerging issues, manifestations and trends with regard to mercenaries and mercenary-related activities and private military and security companies and their impact on human rights, particularly on the right of peoples to self-determination. The group is made up of independent experts each representing a geographical region, and it carries out in-country visits and drafts reports considering the impacts of the activities of mercenaries and other related actors. The Working Group created to support the convention has significantly broadened its activities and approach, looking at the activities of private security companies, and more recently at the use of ICTs in private security activities. Furthermore, as mentioned above, the draft convention on PMSCs that it developed was one of the first documents to explicitly recognize the "transfer of knowledge with security and policing applications" as part of private security services.

Recently, it has been looking at the use of ICTs by private security actors, holding consultations on the activities of "cyber mercenaries", receiving submissions and inputs from a number of civil society, humanitarian and private actors, resulting in a report being presented to the General Assembly on July 2021.[37]

[37] United Nations General Assembly, *The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities - Report of the Working Group on the use of mercenaries*, 15 July 2021, A/76/151 [last accessed 7 July 2022].

South African Private Security Regulation

South Africa has enacted some of the most restrictive extraterritorial legislation on the participation in armed conflict outside its borders of people with ties to South Africa.[38] It also has created The Private Security Industry Regulatory Authority (PSIRA) to oversee the South African private security marketplace.

Recently, South Africa has put cybersecurity in its sights, and is about to release a report on the topic. Using the moniker "Cybersecurity service provider" or CSSP, the report equates cybersecurity with private security, stating that "the new private security industry is called cybersecurity."[39] It goes on to says that in order to bring CSSPs within the remit of the PSIRA, "a person needs to view cyber (internet) as the space in which security services are rendered. Secondly, one needs to treat systems, networks, programs, devices and data as an individual or organisation's belonging."[40] Furthermore, the study goes on to say that "all intrusion software used to prevent cyberattacks form part of this study because their assistance in locating, deciding and controlling unauthorized system behaviour such as unathorised access, or modification and destruction can be regarded as security equipment."[41] Notably, it defines relevant private security services in the following manner:

> The services rendered by PSSPs[42] and CSSPs to their clients include protecting clients or their properties; investigating criminal activities; advising clients on security measures to be implemented in the protection of the property and/or persons; responding or reacting to security breaches; distributing or selling security equipment; training candidates to be security specialists; monitoring signals or transmissions from security equipment; managing, controlling, and supervising the rendering of security services. These service providers render their services in the physical and cyber spaces for remuneration, reward, fee or benefit.[43]

What is remarkable about this study is the explicit recognition that cybersecurity services are private security services, as well as the exercise it undertakes to map "traditional" private security services to the cyber domain in order to bring them within the remit of existing South

[38] *The Regulation of Foreign Military Assistance Act 15 of 1998* (FMA), The Republic of South Africa Government Gazette, 20 May 2998, and its intended replacement, *The Prohibition of Mercenary Activities and Regulation of Certain Activities in Country of Armed Conflict Act 27 of 2006*.

[39] Xulu, Hloniphani, *The new Private Security Industry: Regulating Cybersecurity Services* (2022), p. 2 [not yet published].

[40] Ibid, p. 4

[41] Ibid, p. 14.

[42] The acronym PSSP stands for "Private Security Service Provider".

[43] Ibid., p. 20

African legislation and oversight. At the time of this writing, this study is currently slated to be presented to the South African Parliament towards the end of 2022.

Wassenaar Arrangement (1996)

The Wassenaar Arrangement is a multilateral harmonization arrangement for import and export controls. Unlike its Cold-War era predecessor the Coordinating Committee for Multilateral Export Controls (COCOM), The Wassenaar Arrangement (WA) does not control the items on control lists themselves, rather it harmonizes the control lists for participating states, and then each state implements the control list according to its own fashion. The rationale for the control lists is to prevent "destabilizing accumulations" of products around the world. If an item is on the control list, this doesn't mean it can't be traded, rather it means that it has to be licensed. States notify other Wassenaar states of the licenses they have approved, the sensitivities of items and the licenses that were denied.

Member states participating in the Wassenaar arrangement do not have to report transfers to other member states, resulting in what one expert called a "Catch-22" situation: the more members that are part of the Wassenaar Arrangement, the less transparent import-export controls become. To become a member state, it must be voted on by consensus by the other member states, but there is no procedure for removing a member state, nor has it happened since the Arrangement was established.[44] As such, the Wassenaar Arrangement does little to oversee import-export of potentially human rights violating items, and has no accountability mechanism.

In 2013, after revelations that European companies had sold systems to governments in Syria and Libya enabling those governments to monitor and intercept the electronic communications of their citizens, France and the UK proposed the inclusion of intrusion software and IP surveillance systems on the WA's dual-use control list. According to one expert, the discussions on their inclusion were the first time that the human rights' impacts of dual-use items were discussed within the WA framework, which according to another expert has historically focused on the "double duality" areas of civil-military and "offensive-defensive" characteristics.[45] Furthermore, the inclusion of surveillance technology on the control list highlights its "weaponized" nature and risks for human security.

Import-export controls provide one interesting avenue for restricting the sale of ICTs that can be used to violate human rights, particularly as a WA expert said that "essentially all ICTs are dual-use." However, the current regime which does not have explicit human rights

[44] For more information about how the Wassenaar Arrangement operates, see Evans, Samuel, *Revising Export Control Lists*, Flemish Peace Institute, 24 March 2015 [last accessed 7 July 2022].

[45] Géry, Aude, *Droit international et prolifération des cyberarmes*, « Politique Etrangère » 2018/2 [last accessed 7 July 2022].

protections, and further which lacks transparency for participating states, would need to be redesigned to effectively regulate the trade of products/services that threaten human security.

### Voluntary Principles on Security and Human Rights (VPSHR) (2000)

The VPSHR is one of the early multistakeholder initiatives which brought together stakeholders from governments, multinational extractive companies and civil society organizations to develop human rights guidelines for extractive companies' engagement with both public and private security forces that provide security services to their organizations. The Principles themselves provide guidance to companies on how to carry out risk assessments, as well as how to interact with both public and private security stakeholders.

The Voluntary Principles Initiative (VPI) provides a forum for exchange among the different stakeholder members, who are required to prepare a report each year detailing their efforts to implement the Principles. However, the VPI does not have an oversight or accountability framework, the lack of which has been criticized particularly by members of civil society.[46]

Identifying the increased use of ICTs in security by its members as clients, the VPSHR recently held a panel discussion on the topic at its Annual Plenary in May 2022. Discussions highlighted the increasing use of technologies by PSCs such as surveillance drones and the collection and storage of large amounts of personal and sensitive information, as well as the need to update due diligence considerations for hiring PSCs to include the impacts of their use of ICTs on human rights. This is yet another initiative that is grappling with how ICTs are transforming the delivery of security services, including by private commercial actors.

### Montreux Document (2008)

The Montreux Document is a joint initiative of Swiss government and ICRC which was created in the wake of the proliferation of private security personnel supporting states on the battlefield in the early 2000s. Concerned by reports of wrongdoing of private military and security companies ("PMSCs") within the contexts of the Afghan and Iraqi wars, as well as further claims that such actors provided services outside of the scope of international (humanitarian) law, the initiative undertook to interpret existing international humanitarian law obligations of states regarding PMSCs. To do this, the document organizes state obligations according to the categories of "Contracting States", "Territorial States" and "Home States", or states in which a PMSC has a strong national tie. This innovative approach illustrates how existing international legal obligations can be "updated" to reflect new developments without going through a treaty negotiation process. Furthermore, the Montreux Document lists 73 human-rights-based good practices that States should adopt vis-

[46] From interviews as well as author's own experiences participating in the VPIs

à-vis PMSCs operating in both armed conflict and peacetime and is firmly grounded in human rights law.

As of the time of writing, the Montreux Document has been endorsed by 58 participating states and three international organizations. These states make up the Montreux Document Forum, which meet on a regular basis to discuss topics relevant to the private security industry.[47] However, one of the main limits of the Montreux Document is contextual scope, because it is applicable only in the armed conflicts. This excludes the situations where companies provide security services using ICTs in peace time (migration detention, border management, extractive industry).

Global Network Initiative (2008)

The Global Network Initiative (GNI) is a multistakeholder initiative created with the twin goals of 1) protecting the privacy rights of individuals and 2) preventing Internet censorship by governments. Its members are made up of companies, civil society organizations and universities. Governments do not participate in the initiative because it was felt that this could undermine the objective of undue intrusion into privacy by governments. GNI has developed a set of Principles which aim to “protect and advance freedom of expression and privacy in the Information and Communications Technology (ICT) industry globally”. It acknowledges the companies’ “responsibility to protect and promote the freedom of expression and privacy rights of their users” enjoining them to “avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations” where national laws and practices “do not conform to international standards.”[48]

As such, the GNI Principles puts the onus on the companies to push back against governmental requests and practices that are not in conformance with international human rights treaties,[49] as well as to not enter into commercial agreements with governments that are deemed likely to use ICTs for human rights abuses. While one interviewee commented that this put too much responsibility on companies to essentially be the enforcer of human rights standards even with regards to government practices, others emphasized that companies have great power and responsibility to prevent abuses by governments. GNI member companies are independently assessed every two to three years on their progress in implementing the GNI principles, with the purpose of determining whether a member

[47]For more information, visit the Montreux Document Forum website.

[48] *The GNI Principles,* Global Network Initiative (2008) [last accessed 7 July 2022].

[49] The treaties cited by the GNI Principles include the the Universal Declaration of Human Rights (“UDHR”), the International Covenant on Civil and Political Rights (“ICCPR”) and the International Covenant on Economic, Social and Cultural Rights (“ICESCR”). 2, 3 The application of these Principles is informed by the UN Guiding Principles on Business and Human Rights (“UN Guiding Principles”), the ‘Protect, Respect, and Remedy’ Framework, and the OECD Guidelines for Multinational Enterprises

company is “making good-faith efforts to implement the GNI Principles with improvement over time.”

## International Code of Conduct (2010)

The International Code of Conduct for Private Security Service Providers was launched by the Swiss government as complementary initiative to the Montreux Document to create standards and principles in alignment with human rights standards for private security companies (PSCs). It is another example of translating human rights standards into practical guidance to companies that decreases the likelihood that PSCs’ services will negatively impact human rights and aimed to respond to the challenges of actors operating across borders and in multiple jurisdictions, many of which are in areas of weakened governance, by putting human rights-respecting responsibilities on the companies themselves.

Upholding these responsibilities is overseen by the International Code of Conduct Association (ICoCA), a multistakeholder oversight and governance framework which aims to hold member companies accountable, as well as to provide effective remedies to those whose rights have been negatively impacted by PSC companies. Its governance framework provides equal decision-making authority to governments, PSCs and civil society organizations. This approach to multistakeholder governance recognizes the different areas of “effective control” that governments, companies and civil society have, and encourages them to work together to respect the standards in the ICoC.

While the model has had modest success in attracting PSC and civil society organization (CSO) members, the comparatively small participation of only 7 States demonstrates a certain reluctance of states to be on an “even footing” with other non-state members. Additionally, the total membership of around 230 stakeholders represents a tiny fraction of the members of the sector, although the normative and standard-setting influence arguably reaches beyond those who are actual members.

Recognizing that private security services are increasingly using ICTs, some human rights experts such as former Special Rapporteur on Freedom of Opinion and Expression, David Kaye[50], and the UN Working Group on Business and Human Rights, have specifically identified the ICoC/A initiative as a forum for “operationalizing the human rights responsibilities of the sector, and setting out practical guidance and standards for the responsible provision of

[50] Kaye, David, *Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35, paras. 63-64 last accessed 7 July 2022].

cyberservices."[51] Currently, the ICoCA is looking at the issue of its members using ICTs in their service offerings, including possibly updating its standards and oversight functions to reflect this new reality.

### The United Nations Guiding Principles on Business and Human Rights (UNGPs - 2011)

The UNGPs is an instrument containing 31 principles for implementing the "Protect, Respect and Remedy" framework. Developed under the leadership of Special Representative of the Secretary General (SRSG) John Ruggie, the UNGPs provide guidance to both states and businesses to implement the framework, which articulates 1) the state duty to protect human rights, 2) the corporate responsibility to respect human rights, and 3) access to remedy for victims of business-related human rights abuses.

Importantly, a core component of the UNGPs is that companies are required to carry out robust and continuous *due diligence*, which should include "assessing actual and potential human rights impacts, integrating and acting upon the finding, tracking responses, and communicating how impacts are addressed." Furthermore, this assessment should include identifying potential adverse human rights impacts that the company's activities might cause or contribute to, or which may be "directly linked to its operations, products or services by its business relationships", including its clients.

### B-Tech

In 2019 OHCHR launched the B-Tech project, which aims to apply the "Protect, Respect and Remedy" Framework to the ICT space. In particular, it sets out guidance for due diligence processes to identify, prevent or mitigate risks of harmful impacts if ICTs on human rights. In the case that such harmful impacts do occur, it provides guidance for effective remediation processes. This is another initiative that recognizes the power of the company to provide human-rights respecting services through its selection of clients and contracts.

### UN Normative Framework of Responsible State Behavior in Cyberspace

In 1998 the Russian Federation sponsored a UN General Assembly (UNGA) Resolution on "Developments in the field of information and telecommunications in the context of international security". It was the first of several resolutions that launched workstreams on cyber and security, including six UN Group of Government Expert groups (GGEs) and two Open Ended Working Groups (OEWGs), resulting in the development of the "UN Framework

[51] United Nations General Assembly (UNGA), *Issue of human rights and transnational corporations and other business enterprises, report of the Working Group on the issue of human rights and transnational corporations and other business enterprises*, 21 July 2020, A/75/212., para 97. [last accessed 7 July 2022].

of Responsible State Behaviour in Cyberspace".[52] Consisting of eleven "voluntary, non-binding" norms which aim to guide states in their activities online, it was unanimously endorsed by the UN General Assembly.

The framework can be seen as an attempt to translate international standards and obligations into a format that is better adapted to the information age, and to "increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.[53] Since the framework was first articulated in 2015 by the 4th UN GGE it has been further refined and explained in subsequent GGE and OEWG reports. In October 2020, France and Egypt launched a Program of Action on the International Security Aspects of Information and Communication technologies and responsible State behavior in cyberspace (PoA)[54] inspired by the Small Arms and Light Weapons PoA of 2001, to develop a permanent UN platform for operationalizing the normative Framework. Supported by more than 50 states, the PoA also envisages "meaningful participation" by civil society and companies.

Confidence Building Measures (CBMs)

Confidence Building Measures (CBMs) are actions and processes undertaken to reduce or eliminate causes of mistrust, tensions and hostilities among states that could lead to escalations of tension and conflict.[55] A technique that has been used over the last century, it was used with success as a kind of "pressure valve" to deescalate tensions during the Cold War. CBMs can also act as a precursor to the establishment and reinforcement of international norms.[56] Of note, in addition to supporting the use of CBMs to further develop and strengthen the Responsible Framework of State Behaviour in cyberspace, the final 2021 report of the OEWG noted that "the dialogue within the Open-ended Working Group was itself a CBM" because of the way it stimulates discussion and exchange of ideas.[57]

[52] United Nations General Assembly (UNGA) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, A/70/174 [last accessed 7 July 2022]. Open to all UN member states, the second OEWG was launched in 2021, and is tasked to further develop the UN Normative Framework.

[53] Ibid, Norm 13a.

[54] *Program of Action on the International Security Aspects of Information and Communication technologies and responsible State behavior in cyberspace* [last accessed 7 July 2022].

[55] For more information about CBMs in cyberspace, see Stauffacher, Daniel & Kavanagh, Camino, *Confidence Building measures and International Cyber Security*, ICT4Peace Foundation (2013), [last accessed 7 July 2022].

[56] *Overview of Existing Confidence Building Measures as Applied to Cyberspace*, GFCE, 03/06/20, *p*.7 [last accessed 7 July 2022].

[57] United Nations General Assembly (UNGA), *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security*, 10 March 2021, A/AC.290/2021/CRP.2, para. 43 [last accessed 7 July 2022].

Interestingly, regional organizations have prioritized developing CBMs to reduce the risks of conflict from the use of ICTs, including ASEAN, OAS and the Organization for Security and Cooperation in Europe (OSCE). In particular, OSCE has developed 16 CBMS, as well as tools and mechanism to deescalate tensions and avoid misunderstandings. These tools include:

- Consultation mechanisms to de-escalate rising tensions by bringing states together over potential cyber/ICT security incidents;
- A platform for exchanging views, national cyber/ICT security policies and approaches to allow states to better "read" each other's intentions in cyberspace; and
- Concrete work items for participating States to collectively enhance cyber resilience in the OSCE region for the benefit of all.

Finally, some of the multistakeholder governance initiatives involving states mentioned in this section could also be called a kind of CBM insofar as they can help build trust and deescalate tensions through mechanisms involving both state and nonstate actors.

### The Digital Geneva Convention

In 2017, Microsoft President Brad Smith took up a cause to bring international law to attacks in cyberspace. Authoring a blog on the Microsoft website and speaking at several international conferences, including an address to the United Nations at Geneva in November 2017, Smith proclaimed 'The need for a Digital Geneva Convention.' Citing the alarming growth of not only cybercrime, but also the proliferation of attacks on nation states, Smith called on governments to 'implement international rules to protect the civilian use of the internet.' Using language clearly inspired by the 1949 Geneva Conventions, Smith offered 6 principles to guide such a convention, calling on states to 1) not target tech companies, private sector, or critical infrastructure; 2) assist private sector efforts to detect, contain, respond to, and recover from events; 3) report vulnerabilities to vendors rather than to stockpile, sell or exploit them; 4) exercise restraint in developing cyber weapons and ensure that any developed are limited, precise and reusable; 5) commit to non-proliferation activities for cyberweapons; and 6) limit offensive operations to avoid a mass event.[58]

While not completely novel[59], the approach was both welcomed as timely and criticized as wrong-headed, with critics saying that a private company – even one as large and influential as Microsoft – was not the right actor to launch an initiative that was destined for states. Other stakeholders commented on the lack of an inclusive process for developing the Digital Geneva Convention, feeling that the principles had been declared without the possibility to

[58] Smith, Brad, *The need for a Digital Geneva Convention*, 14 February 2017 [last accessed 7 July 2022]

[59] In 2011, ICT4Peace Foundation called for an "International Code of Conduct on Cyber-Conflict", to set out standards for how states should behave in peacetime and wartime. The proposed Code of Conduct was grounded in the principle that "a cyber-attack on another state is a break of international law."

help develop or influence them. After several months of seeking the spotlight, the initiative seemed to revert to the background while Microsoft set its sights on other, less contentious avenues such as the Cyber Tech Accord and the Paris Call.

However, the idea of translating Henri Dunant's principles into the digital realm did not entirely go away, with publications from the World Economic Forum (2017), Foreign Policy Magazine (2018), the Atlantic Council (2019), National Defense Magazine (2020) and the Lawfare Blog (August 2021) advocating for work to be done in this area.[60] Furthermore, the 2022 conflict in Ukraine in which cyberattacks have been launched along with kinetic attacks (see Spotlight on the Ukraine war below) arguably puts the Digital Geneva Convention in a new light. As such, there may now be more support to take another look at how to translate the principles and obligations of IHL, such as in a more inclusive multistakeholder process similar to the Montreux Document or the ICoC.

### Paris Call

Launched in November 2018 at the Internet Governance Forum (IGF) held in Paris by French President Emmanuel Macron with strong support of Microsoft, the Paris Call set out 9 principles for members of governments, civil society and commercial actors to promote "Trust and Security in Cyberspace,"[61] and which touch on many of the security and human rights aspects relevant to private actors using ICTs in their security services.[62]

As of this writing, the multistakeholder initiative has been endorsed by 81 States, 36 public authorities/local governments, 390 Civil Society Organizations and 706 companies, for a total of over 1200 supporters. The Call has provided a forum of discussion on matters related to trust and security in cyberspace for both state and non-state stakeholders alike. In 2021, it launched 6 working groups to work on areas of ICT threats and opportunities, with a view to feeding the findings into operationalizing the above-mentioned PoA. While the Call has steadily increased its membership, with the US and the European Union joining in 2021, some states have not joined the Call, including Russia and China.

### Other relevant initiatives

Other initiatives which are relevant to ICTs and human security include:

- *The Internet Governance Forum (IGF):* a multistakeholder governance group that discusses issues of internet governance. Launched by UN Secretary General Kofi

[60] Lohrmann, Dan, *The Case for Establishing a Digital Geneva Convention* Government Technology, 8 August 2021 [last accessed 7 July 2022].
[61] *The 9 Principles*, Paris Call Initiative (2018) last accessed 7 July 2022].
[62] From the Cyber Tech Accord website, last accessed 7 July 2022.

Annan in July 2006, it convenes an annual meeting holding hundreds of workshops on topics ranging from expanding Internet access, preventing hate speech online, protecting the rule of law online and building internet capacity.

- *The Freedom Online Coalition (FOC):* brings together 34 governments supported by a multistakeholder Advisory Network working towards advancing internet freedom. The FOC issues Joint Statements articulating global norms for the Internet, organizes an annual event and coordinates diplomatic interventions and initiatives in different international fora.

- *The Cyber Tech Accord:* launched in 2018 under Microsoft's leadership, the Cyber Tech Accord is made up of over 150 companies which publish reports, white papers, case studies and policy submissions with the aim to improve "the security, stability and resilience of cyberspace". Members commit to the Accord's four core principles: 1) Strong defense, 2 No offense, 3) Capacity Building and 4) Collective response.[63]

- *The Siemens Charter of Trust:* launched in 2018 at the Munich Security Conference, the Siemens Charter of Trust brings together 17 companies (not all of the ICT companies) and 11 members from government and civil society to secure the ICT supply chain. The Charter has three primary objectives: 1) protect the data of individuals and companies, 2) prevent damage to people, companies and infrastructures, and 3) create a reliable foundation on which confidence in a networked world can grow. Members commit to respect 10 principles fundamental to a secure digital world.

- *Global Forum Cybersecurity Expertise (GFCE):* launched in 2015 at the Global Conference on Cyber Space in the Hague, GFCE is a clearinghouse and platform for coordinating cyber capacity building offerings throughout the world. It aims to implement a "Global Cyber Capacity Building Research Agenda" to fill cybersecurity knowledge gaps and capacity needs.[64]

- *RightsCon:* is an annual conference dedicated to protection of human rights in the digital space. It bills itself as "a civil society-led space where all stakeholders—from tech companies to government representatives to human rights defenders" can work together to "build a rights-respecting digital future." The first conference was held in 2011 in Silicon Valley by the organization Access Now.[65]

[64] For more information, visit the GFCE website, last accessed 7 July 2022.
[65] More information about RightsCon can be found on its website, last accessed 7 July 2022.

## Mapping the use of ICTs in private security services provided by commercial actors

Building on the previous discussions, this section will provide a high-level mapping of security services falling in the following two categories:

1) Services that use ICTs to protect/defend persons and objects
2) Services that use ICTs to gather and analyze information for security purposes

The first section of services reflects actual service and products currently offered by ICoCA member companies, as identified through research of company websites, other online sources, interviews with company representatives and clients, as well as workshops with ICoCA members. This is followed by a section on services that match the above criteria but were not found through the above methods to be provided by ICoCA member companies. The final section will take a closer look at private ICT commercial actor involvement in the Ukraine war.

As new ICT offerings are continuously being added to the marketplace, the study does not purport to present all relevant services, but represents those which experts found most important/concerning at the time the research was carried out.

### From boots on the ground to bytes in cyberspace: security services utilizing ICTs offered by private commercial actors including current ICoCA members

Through research and interviews with ICoCA member companies, it was ascertained that at least **61 ICoCA member companies** of the 89 companies reviewed[66], or **68.5%,** provide at least one of the services below, the vast majority providing more than one of them. Surveillance/remote monitoring using CCTV was the most provided service, with at least 28 companies explicitly offering this service. This was followed by intelligence services which saw at least 18 PSC providing these services. At least 10 ICoCA member companies provide cybersecurity services. Several member companies noted a significant increase in and shift to utilizing ICTs in their provision of security services over the past 5-7 years, with the Covid-19 pandemic accelerating this shift, and the outlook that this will only continue to be on the rise.[67] Members described creating new divisions within their company or even new company spinoffs devoted to ICT-focused services.

#### *Video surveillance CCTV*

The use of video surveillance cameras by companies to provide security services is not a new phenomenon. What is new are the capabilities of the video cameras that are now available

[66] As of 12 May 2022. The discrepancy between this number and the ICoCA company membership number is due to websites being down/lack of information provided by company,

[67] Quantitative analysis carried out through a key-word query of LinkedIn companies identified nearly ten thousand companies worldwide carrying out these services. For more information, see Annex II.

on the market, and the kinds of information they are capturing. These new features include: facial recognition, silhouette recognition, and vehicle recognition. Silhouette recognition technology is said to create a unique "silhouette profile" based on a person's based on height, size, clothing, and other factors to track movements when a subject's face is not visible. Other filters can be included to carry out data searches according to age, gender or race. Video surveillance is partculary used in the context of border management and migration. [68]

Case Study: Anduril's Lattice platform powers surveillance at US borders

Anduril Industries was awarded a $13.5 million USD contract to provide fully autonomous surveillance capabilities at military bases that are located near the US-Mexico border. The system known as Lattice detects motion, focuses its cameras on the location, and then uses computer-vision algorithms to determine what is causing the motion, with the ability to distinguish between humans and human-driven vehicles and animals or other objects. The technology enables one person to "keep watch over hundreds of miles of terrain."[69] Through Freedom of Information Requests to the US government, the advocacy organization Mijente reported on the contracted services, stating that the "algorithms are trained to implement racist and xenophobic policies."[70] The UN Working Group on the use of Mercenaries also expressed concern about human rights violations being committed by use of ICT-enabled surveillance capabilities at borders.[71]

### *Securing ICS/SCADA devices*

Industrial control systems/supervisory control and data acquisition (ICS/SCADA) are typically used to secure critical infrastructure installation systems (CIIs) that provide water, electricity, manufacturing, transportation, banking and other critical services.[72] If the ICS/SCADA systems of critical infrastructure installations are brought down or compromised, this can have catastrophic results for the societies that depend upon them, including injury, instability and uprisings, serious health consequences aAnothend death.

Recognizing the important humanitarian and societal consequences of these devices, several initiatives and organizations have called on states and other actors to refrain from cyber attacking these systems that protect CIIs, including the organization preparing this study

[68] United Nations Human Rights Council (HRC), *Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants*, 9 July 2020, A/HRC/45/9 [last accessed 7 July 2022].

[69] Ward, Jacob and Sottile, Chiara, *Inside Anduril, the startup that is building AI-powered military technology*, 3 October 2019, NBC News, [last accessed 7 July 2022.]

[70] Mijente, *Anduril's New Border Surveillance Contract with the US Marine Corps and CBP*, 24 July 2019, [last accessed 7 July 2022].

[71] See, e.g., United Nations Human Rights Council (HRC), *Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants*, 9 July 2020, A/HRC/45/9 [last accessed 7 July 2022].

[72] Fortinet, "What is ICS Security" [last accessed 27 July 2022].

ICT4Peace Foundation[73], the Paris Call, the ICRC and the UNGGE and OEWG in their development of and support for the normative framework for responsible state behaviour in cyberspace.

*Location Tracking*

Location tracking services provide real-time monitoring of persons and vehicles. Typically used in areas that are high-risk for kidnapping, robbery and other acts of violence, these services make use of wireless technologies such as satellite, GSM (3G/4G/5G), and sometimes shorter range wireless networks to track people's movements. The persons movements are tracked either by devices that are mounted in vehicles[74], or increasingly by smartphone apps, which a number of companies are now developing.[75]

Location tracking can interfere with the right to privacy, as it captures and records persons' movements, however this is not a violation so long as the concerned persons are aware of the tracking and have meaningfully consented to it. What is more problematic is when ICTs are used to track location and movement of persons without their knowledge and consent, as will be discussed further below.

*Drones*

Unmaned Arial Vehicles (UAV), otherwise known as Drones, provide surveillance and other security functions from overhead. These unmanned flying machines are equipped with multiple capabilities, including high definition cameras, often equipped with facial recognition technology, and thermal cameras equipped with body heat sensors, lights, comms, lidar, electronic payload options and can also be used to fire weapons. Some of them have autonomous capabilities, meaning they can fly without humans piloting them.[76] A recent UN report by the UN Panel of Experts on Libya[77] detailed a March 2020 skirmish in which such a drone, also known in academic parlance as a lethal autonomous weapons system or LAWS, made an appearance on the battlefield. These aircrafts are used for a variety of different functions, including perimeter security, reconnaissance, aerial mapping and in conflicts.[78]

[73] ICT4Peace Foundation, *Critical Infrastructure and Offensive Cyber Operations, A Call to Governments*, 30 November 2019 [last accessed 27 July 2022]

[74] Interview with private security company.

[75] Interview with private security company.

[76] Nichols, Greg, *The 5 best surveillance drones: Next-level inspection UAVs, ZDNet,* 20 May 2022 [last accessed 27 July 2022]

[77] United Nations Security Council (UNSC) "Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, UN, 8 March 2021 [last accessed 7 July 2022].

[78] Korkmaz, Emre Eren, *Refugees are at risk from dystopian ¨smart border" technology*, 8 December 2020 [last accessed 7 July 2022].

Case Study: Use of drones by private companies hired by Frontex to monitor migrants on Mediterranean[79]

On 20 October 2020, *The Guardian* reported that Frontex, the European Border and Coast Guard Agency, had awarded contracts to Airbus and Israeli Company Elbit Systems Ltd. to patrol migrant boats crossing the Mediterranean.[80] It was later reported that this aerial footage was routinely shared with the Libyan Coast Guard, who would intercept the boats even though they were well out of Libyan waters, and forcibly return them to Libya, where the migrants were held in detention centers. According to one legal expert, this has been done routinely in violation of international law which would require European officials to first make a determination of whether the migrants would qualify for refugee status, as well as to determine that sending them back to a jurisdiction where they would face torture, cruel, inhuman or degrading treatment or punishment and other irreparable harm (the principle of non-refoulement). Migrants that were captured by Libyan coast guard officials reported that they had been beaten, and there were other reports that a migrant was shot and killed in a Libyan detention center.[81] There have also been reports on the use of drones at the US-Mexico border to track would-be migrants, including using AI and facial recognition technology.[82]

*Access Control*

Access control systems secure physical premises, controlling which user can go where and when, as well as creating a record of the comings and goings of people to which areas. Typically, these systems use a software-driven control center which is monitored remotely. Access is controlled via a variety of different means, including Radio Frequency Identification (RFID) cards, smartphone applications and biometrics, including facial recognition, fingerprint and iris scans.[83] These systems record the comings and goings of people, including time stamps on ingress and egress, and their whereabouts. Those systems that use biometrics for identification also capture and store very personal information, such as fingerprints and iris scans.

*Security Apps*

SOS Apps are smartphone apps supported by private security services which provide users a "panic button" to report when they find themselves in an emergency. The apps then use wireless location tracking technology to find out where the user is and send assistance. Typically, users will be able to choose from different "panic buttons", e.g., security

[79] Mazzeo, Antonio "Border surveillance, drones and militarization of the Mediterranean", *Statewatch,* 6 May 2021 [last accessed 7 July 2022].

[80] Jolly, Jasper, "Airbus to operate drones searching for migrants crossing the Mediterranean", *The Guardian,* 20 October 2020, [last accessed 7 July 2022].

[81] Urbina, Ian, "Europe's border agency under fire for aiding Libya's brutal migrant detentions", NBC News, 29 November 2021 [last accessed 7 July 2022].

[82] Ibid.

[83] DeMuro, Jonas, "Best access control systems of 2022", Techradar, 19 May 2022 [last accessed 7 July 2022].

emergency, medical emergency or roadside emergency. The response sent by the security company will depend upon the kind of emergency selected. For example, if a security emergency is sent, then the company will send its nearest rapid response team, if it is a medical emergency, then ambulance services will be sent.

*Intelligence Services*

Signals Intelligence, otherwise known as SIGINT, denotes the collection of messages and data via electronic communications (COMINT)  and/or electromagnetic emissions of aerospace, surface and subsurface systems. SIGINT can include verbal communications, written messages, data from radar or weapons systems. Open Source Intelligence (OSINT) is the collection of publicly-available material. The kinds of information that can be found are quite diverse, and can include postings on social media platforms as well as location information leaked by advertisements on smartphone apps.[84] "Automated OSINT" uses software that queries multiple online sources of data simultaneously, which are aggregated by vendors into a single searchable source which can contain billions of records.[85] According to the Dutch Review Committee on the Intelligence and Security Services,

> *The volume, nature and range of personal data in these automated OSINT tools may lead to a more serious violation of fundamental rights, in particular the right to privacy, than consulting data from publicly accessible online information sources, such as publicly accessible social media data or data retrieved using a generic search engine.*

Automated OSINT services can be accessed through a number of online portals and apps.[86]

Case Study: US Military bypasses judicial supervision by purchasing location information from third party broker

The New York Times reported that US military agencies were buying mobile phone location data from third-party brokers to trace past movements of users without judicial supervision. This is done even though a 2018 Supreme Court ruling found that the US Constitution's protections against "unreasonable searches and seizures" required governmental officials to get a judicial warrant in order to obtain the same information directly from phone

[84] Oerlemans, Jan-Japp, "Privacy risks of (automated) Open Source Intelligence (OSINT)", About Intel [last accessed 7 July 2022].

[85] "Summary of Report No. 74 regarding automated OSINT by the Dutch Committee on the Intelligence and Services", Dutch Review Committee on the Intelligence and Security Services, 08 February 2022, [last accessed 7 July 2022].

[86] Sharma, Ax, Breeden II, John and Fruhlinger, Josh, "15 top open-source intelligence tools", CSO online, 28 June 2021 [last accessed 7 July 2022].

companies.[87] Mobile phone companies routinely sell this information to third party brokers who then typically sell it to advertisers for marketing purposes. Because this information is freely available on the market, US military officials maintain that they should also be able to buy this information, even though it is used for law enforcement purposes.

*Threat Assessment Reports*

Threat assessment reports, also known as, risk intelligence reports identify potential threats in a particular area or venue and evaluate the likelihood of the occurrence of the threat. Companies providing these services typically undertake the following steps: 1) a threat assessment that looks at natural threats, criminal threats, terrorist threats and potential accidents; and then carries out a 2) vulnerability assessment which makes a determination of the assets at risk (e.g., people, equipment, physical premises) as well as an assessment of the attractiveness of the assets as targets, as well as the defenses against threat that already exist. Companies often use software platforms to carry out these threat assessments, which include artificial intelligence (AI) and use of intelligence gathering methods described in the previous sections.

*Cybersecurity services*

Securing computers, machines, networked devices and the software that operates the are the services most commonly associated with cybersecurity, and it's a field in which ICoCA member companies are increasingly getting into.[88]

The National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022 defines cybersecurity as a:" [d]esirable state within cyberspace in which communication and data exchange between information and communication infrastructures function as originally intended. This state is achieved with measures of information security and cyber defence."[89]

The US National Institute of Standard and Technology (NIST) defines cybersecurity as:

> *[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*

[87] Savage, Charlie, "Intelligence Analysts use US Smartphone Location Data without Warrants, Memo Says", *New York Times*, 22 January 2021 [last accessed 7 July 2022].

[88] A review of the security services ICoCA member companies listed on their websites found that at least thirteen ICoCA member companies are providing these services

[89] National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022, p. 31.

These services typically are offered to defend ICTs from attacks, as well as to secure data located within those systems. So-called "passive cyber defense services", they involve analyzing the traffic on a network over a period of time to identify vulnerabilities and malware infections. They then will provide a report on the findings and provide recommendations to respond to security threats. "Active cyber defense" services refer to services in which a security company is in a client's computer systems and proactively guards against intruders into their computer systems. The services may include "hacking back"[90], controversial activities in which the attacker's computer system is accessed in retaliation, and which is illegal in many jurisdictions.

*Digital forensics*

Digital Forensics denotes processes to uncover, identify, extract, and document evidence after a cybersecurity or data breach incident. It examines cybersecurity incidents within the ICT architecture and detects the digital footprint left by the attacker, with a view to identifying vulnerabilities that allowed the attack as well as the origin/author of the attack. There are many different branches of digital forensics, which include malware forensics, database forensics, browser forensics, dark web forensics, and newer areas such as Internet of Things (IoT) forensics. Companies providing these services often collaborate with law enforcement officials in investigations of cyber incidents.

In carrying out digital forensics, a number of kinds of information can be used in the identification of the digital footprint, including examining meta data and other file logs, "file artifacts" or data that is generated when, for example, a file is created, or other evidence that efforts were undertaken to hide or change information, such as by changing the time on the computer clock. Encryption of files can prove challenging to digital forensics, with democratic states divided over whether an individual can be compelled to hand over passwords to law enforcement professionals.[91]

Recently, there has been a push by civil society organiizations such as Amnesty International to increase digital forensics capabilities among human rights defenders in order to carry out technical investigations of cyberattacks against civil society and to provide defensive support when such attacks take place.[92]

## I. Other relevant services

[90] "Hack backs" entail launching a counterstrike against a cyber attacker that can include deleting or retrieving stolen data, identifying the hacker and reporting this to law enforcement authorities, or even harming the attacker's computer system.

[91] Diab, Robert, "Compelling people to reveal their passwords is posing a challenge to police and courts", *The Conversation,* 22 May 2019 [last accessed 7 July 2022].

[92] https://www.amnesty.org/en/latest/research/2022/06/digital-forensics-fellowship/

These services go to those that are similar to the ones above, but which were not in fact found to be currently provided by ICoCA members. Nevertheless, the author does not rule out that these services are currently provided by ICoCA members, only that research of and replies from member companies did not find any instances. Furthermore, given the fast pace of technological and marketplace evolution, it is likely that many of these services will be offered by ICoCA members in the near future.

*Automotive Cybersecurity*

Automotive cybersecurity is the protection of automotive electronic systems, communications networks, software and control networks, and users and their underlying data from malicious attacks. In automotive parlance, the "four ACES disruptions—autonomous driving, connected cars, electric vehicles and shared mobility"[93] have been shaping the auto industry in recent years, turning cars into collectors and repositories of huge amounts of often very personal information. Attacks on cars have been on the rise[94], including large-scale attacks on Toyotas where 3.1 million users' information was stolen[95], and the internet is full of YouTube videos and websites showing how to hack into and take over car control systems, even remotely.[96] The McKinsey Center for Future Mobility expects the market for automotive cybersecurity to reach nearly USD $10 billion by 2030.[97]

*Robots*

The use of robots to carry out security functions including perimeter guarding and intelligence gathering, using technologies such as facial recognition and artificial intelligence.

Case Study: National University of Singapore & Oscar the Robot

Oscar the Robot is part of Certis-Cisco's "Smart Network Security" offering, which combines robots working with specially trained security personnel. Certis claims that the Smart Network Security system increases human security officer productivity by 25% by allowing them to "perform higher value tasks." Oscar the Robot, and its companion Crystal the Concierge Robot, use technologies including facial recognition and artificial intelligence to provide "heightened situational awareness" as well as identification of "undesirable behaviours" such as smoking in non-designated places or overcrowding.

[93] McKinsey Center for Future Mobility, *Cybersecurity in automotive. Mastering the Challenge*, 22 June 2020, p.4 [last accessed 7 July 2022].

[94] See, e.g., the Israeli-based firm Upstream's website, which tracks cyberattacks on cars [last accessed 7 July 2022].

[95] Cimpanu, Catalin, "Toyota announces second security breach in the last five weeks", ZDNet, 29 March 2019[last accessed 7 July 2022].

[96] *Security Magazine*, "How Hackers Exploit Automotive Software to Overtake Cars", 31 October 2019 [last accessed 7 July 2022].

[97] Mckinsey Center for Future Mobility, p.4.

Certis-Cisco was awarded a security contract deploying Oscar the Robot at the residences of the National University of Singapore. Following some privacy concerns from residents about Oscar the Robot, the management company requested more information about the robot from Campus Emergency & Security to share more information on the robot's purposes and objectives. In its response, Certis stated:

> *Oscar is an autonomous robot which Certis has introduced as a Proof of Value Trial. The robot is equipped with Artificial Intelligence to detect unattended bicycles and bags and also project security presence. Do note that there will be no capturing of facial images during the trial.*

Residents expressed their discomfort with the robot on campus, citing privacy concerns, and Oscar the robot was removed from the campus. Nevertheless, university officials are planning to redeploy Oscar the robot in the near future.

*Surveillance Tech*

ICTs are increasingly used to gather information ostensibly to prevent security threats, such as terrorism or crime. So-called "mercenary spyware"[98] has increasingly been in the headlines as it has been found on the phones of journalists and government critics, among others. Mercenary spyware is software that can read information and communications on smartphones and avoids security features such as end-to end encryption by accessing the data before it is encrypted. While in many cases, users have to click on a link included in a message sent on a messaging service or email for the surveillance software to be installed, the development of "zero-click" products such as NSO's Pegasus software means that there is no action required on the part of the smartphone user for the program to be installed on the phone; rather it exploits security vulnerabilities in the smartphone to install itself secretly.[99]

NSO is not the only company engaged in surveillance tech and spyware. In December 2021 Meta, formerly known as Facebook, published a report in which identified four more "cyber mercenaries" from Israel, as well as other companies based in India, North Macedonia and China.[100] Citizen Lab, based at the Munk School of the University of Toronto, has carried out extensive investigations on the uses of surveillance or mercenary tech, and has documented

[98] Many actors have called this kind of technology "mercenary" or "mercenary spyware", including Citizenlab, which has carried out extensive research and reporting on this phenomenon, e.g., Deibert"CatalanGate, Extensive Mercenary Spyware Operation against Catalans using Pegasus and Candiru" 18 April 2022. Other actors include Microsoft, e.g., "Microsoft Blasts NSO Group as Ruthless Cyber Mercenaries Hiding Behind Immunity Shields", 22 December 2020, , and Apple, e.g., "Apple sues NSO Group to curb the abuse of state-sponsored spyware", 23 November 2021. Both companies have sued the Israeli company NSO.

[99] For example, see Apple's report on "NSO Group's Forcedentry Exploit", 23 November 2021.

[100] Gallager, Ryan, "Meta identifies 6 firms, including India's BellTrox, for "indiscriminate" surveillance", *The Print*, 17 December 2021 [last accessed 7 July 2022].

its use on dozens of activists, journalists, government officials and opposition leaders.[101] According to one expert, there are over 200 "spyware" companies who are selling their exploits on the open market.[102] Several organizations[103] and experts including Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance Tendayi Achiume and former Special Rapporteur David Kaye[104] have called for a moratorium on the selling of spyware until "until rigorous human rights safeguards are adopted to regulate such practices and guarantee that governments and nonstate actors don't abuse these capabilities"[105].

Case Study : Targeted Digital Surveillance

A collaborative investigation involving more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories and provided technical support from Amnesty International found widespread use by states of targeted digital surveillance tools on journalists, human rights defenders, lawyers, politicians and other activists all over the world.[106] NSO Group, the Israeli company producing the surveillance tools, states that the "sole purpose of NSO is to provide technology to licensed government intelligence and law enforcement agencies to help them fight terrorism and serious crime,"[107] and asserts that it respects human rights in line with the UN Guiding Principles on Business and Human Rights[108]. However, this is brought into question by its claim that it supplies its clients without actually carrying out due diligence measures to verify end use due to supposedly overriding "national security" interests.[109] The European Parliament established a committee to investigate the use of Pegasus and equivalent software, which held its constitutive meeting on 19 April 2022. The committee is expected to submit a report after 12 months.[110]

[101] Ibid.

[102] See also the "Big Black Book of Electronic Surveillance" which explores surveillance technologies used by governments including the United States, Russia, China, Israel, india, France, Germany and the United Kingdom, as well as listing 150 top surveillance tech companies, [last accessed 7 July 2022].

[103] *UN News,* "Spyware: Rights experts push for surveillance technology moratorium", 12 August 2021 [last accessed 7 July 2022].

[104] *UN News,* "Moritorium call on surveillance technology to end 'free-for-all' abuses", 25 June 2019 [last accessed 7 July 2022].

[105] Duguin, Stéphane, "Renewed call for moritorium on sale and use of spyware", Cyber Peace Institute, 25 May 2022 [last accessed 7 July 2022].

[106] Amnesty International, "Uncovering the Iceberg, the Digital Surveillance Wrought by States and the Private Sector", (2021) [last accessed 7 July 2022].

[107] Ibid, quoting NSO Group, "NSO Group Statement on Facebook Lawsuit", CISION PR Newswire, 30 October 2019. See also NSO Group, Transparency and Responsibility Report 2021, 30 June 2021,, excerpt of Contract Provisions at p. 31: "The end user hereby represents and warrants that it and its respective employees and agents: . . . (iii) shall use the System only for the legitimate and lawful prevention and investigation of serious crimes and terrorism, as defined in Exhibit F or in domestic law in a manner substantially similar to Exhibit F, with the definitions in Exhibit F controlling in cases of any material conflict between the definition of such crimes in domestic law and Exhibit F[.]". [last accessed 7 July 2022].

[108] Ibid.

[109] Ibid., quoting NSO Group, Transparency and Responsibility Report 2021, pp. 9-10.

[110] European Parliament News, "EP inquiry committee for Pegasus and other spyware launched", 19 April 2022 [last accessed 27 July 2022].

In addition to software exploits, telecom companies, communications and equipment vendors have been instrumentalized to carry out surveillance, sometimes on a widespread basis. This includes selling equipment and services which provide access to communications data and information, including audio recordings of conversations.

Case Study: Nokia in Russia
The Finnish company Nokia pulled out of Russia after its invasion of Ukraine in early 2021, however it left behind equipment and software that connected Russia's largest telecommunications network MTS to a powerful surveillance system, called the System for Operative Investigative Activities, or SORM. The SORM is able to listen in on phone conversations, intercept emails and text messages, and track other internet communications. For more than five years, Nokia provided equipment and services to design, optimize and provide service support the connection of the SORM to the MTS network. According to the New York Times, the SORM was used to track supporters of Russian opposition leader Aleksei Nalvany, and intercepted calls of a Kremlin critic who was subsequently assassinated. In addition to Russia, Nokia has also come under criticism for partnering with German company Siemens to install what is termed as "lawful intercept" systems in Bahrain[111] and Iran[112] which were said to have contributed to the torture and imprisonment of dissidents.[113]

Nokia says that it follows international standards that guide core network equipment used for government surveillance. This is understood to mean they have followed the standards contained in the Wassenaar Arrangement.[114] However, as mentioned above, the Wassenaar Arrangement is not an oversight / accountability framework, does not prohibit sales of equipment, and only requires licensing for certain categories of items found on the control lists. Additionally, as both Finland and Russia are members of the Wassenaar Arrangement, there is no requirement on the behalf of either side to report the import-export of such equipment between the two countries. This highlights the "Catch-22" of lack of transparency situation that becoming a member of the Arrangement effectively conveys to its members, and emphasizes the outdated nature of the Arrangement, as well as its lack of human rights protections. Preventing "destabilizing accumulations" of weapons and dual-use goods makes little sense in the case of cyberweapons, which require little beyond common computers and the knowledge to write code. Furthermore, as one expert on the Wassenaar Arrangement

[111] Zetter, Kim, "Nokia-Siemens Spy Tools Aid Police Torture in Bahrain", *Wired Magazine,* 23 August 2011 [last accessed 27 July 2022].

[112] Crawford, David and Fuhrmans, Vanessa, "Siemens Business Surges in Iran", *The Wall Street Journal*, 5 April 2011 [last accessed 7 July 2022].

[113] UpGuard, "Telecommunications Breakdown: How Russian Telco Infrastructure was Exposed", 18 September 2019 [last accessed 7 July 2022].

[114] The author tried to get confirmation from Nokia on this statement but did not get an answer. Consultations with other experts familiar with the matter confirmed that this is what Nokia likely met.

said, nearly all ICTs are "inherently dual-use" because they can be used to capture/transmit information and control/damage ICT systems in ways that pose threats to (human) security.

*Big Data Analytics*

Big data analytics describes the science in which raw data is analyzed in order to find trends and answer questions. It involves collecting, inspecting, cleaning, summarizing and interpreting collections of related information in order to find patterns.[115] The kinds of processes and algorithms are similar to the processes described under SIGINT and OSINT above, however the distinction drawn here is between publicly-accessible communications, data and datasets, and proprietary datasets provided by clients. These client-provided datasets may come from police departments, military defense departments, large financial firms, energy companies or telecommunication companies, to name a few.

Case Study: Palantir and Policing

Palantir Technologies was founded in 2003 as a response to 9-11, and the realization that there had been "all of this information sitting in different silos in US agencies that could have prevented" the attack. Its funding was provided in part by Q-tel, the US Central Inteligence Agency's (CIA) venture-capital arm. Its clients include large defense institutions such as the US Army, US Navy and CIA, and companies like IBM, Amazon and Airbus. Credit Suisse uses Palantir technology to combat money laundering and financial fraud.[116] Two large US police departments, the New York Police Department and the Los Angeles Police Department have also used Palantir in what is known as "data-driven policing," which merges data from crime and arrest reports, automated license plate readers, rap sheets, and other sources. This has provoked criticism from civil liberties organizations around its use leading to invasion of privacy and racial profiling.[117] For example, in late 2014, the NYPD used Palantir's analysis to plan a sting that put rapper Bobby Shmurda in jail.[118]

In response, Palantir states that they do not collect or broker the information themselves, and instead only analyze data that is provided to them by their clients, most of which are government entities. According to one company representative, "Palantir was just the cars, not the ones carrying out the raid."[119] However, this analogy does not take into consideration the importance of the analyzed information or how it may violate privacy and other human rights concerns.

*Weaponization of Information*

[115] Interview with company representative

[116] Finews.com, "Credit Suisse leans into Palantir", 15 November 2018 [last accessed 7 July 2022].

[117] Hvistendahl, Mara, "How the LAPD and Palantir use Data to Justify Racist Policing", *The Intercept,* 30 January 2021 [last accessed 7 July 2022].

[118] Parascandola, Rocco and Moor, Tina, "Brooklyn rapper Bobby Shmurda arrested in gun, narcotics investigation", *Daily News,* 18 December 2014 [last accessed 7 July].

[119] Interview with company representative

Companies that generate disinformation and other divisive content for political ends, also known as "Troll Farms", or "Keyboard Armies", are on the rise. Often hired by governments, these companies post content on social media platforms with a view to spreading propaganda or create division, often with an overarching goal to interfere into the internal affairs of / destabilize another country. However, they are also used by a government against its own population. A 2017 report documented 18 different elections in which Troll Farms attempted to sway the results.[120]

Troll Farms identify real tensions in a population, and then try to insert themselves into the debates with the objective of inflaming them and causing division. Rather than promote one side of an issue, they typically will instead exploit social media algorithms that favor more emotional posts from many sides, and post inflammatory content that is then more likely to "go viral", or be widely shared

Case Study : The Internet Research Agency (IRA)
The Internet Research Agency (IRA) was founded in mid 2013 in St. Petersburg, Russia and is linked to Russian oligarch Yevgeny Prigozhin. Known in Russian slang as the "Trolls from Olgino", the term has come to denote organizations who spread disinformation, or "Troll Farms" (see above). The IRA has been accused of creating Russian disinformation to support its actions in Ukraine, as well as influencing the 2016 US Presidential election in favor of Donald Trump. It was indicted by a US grand jury in 2018 on charges of intent to "interfere with U.S. elections and political processes". According to investigative journalist reports and former employees, the main areas of disinformation for the IRA have been:

- Criticism of Alexei Navalny and his supporters, as well as internal Russian critics in general
- Criticism of Ukraine's and the US's foreign policies, as well as the top politicians of these states
- Praise for Vladimir Putin and his policies in the Russian Federation
- Praise for and defense of Bashar al-Assad, the President of Syria

In addition, the IRA has spread disinformation campaigns in order to sow distrust and division in American political and media institutions, as well as to foster Russian public support for the war in Ukraine.[121]

## II. Focus : The War in Ukraine

On 24 February 2022, Russia invaded Ukraine. While some reporters have commented on the apparent lack of cyberwarfare during the conflict[122], reports that have been published by

[120] Freedom House, "Manipulating Social Media to Undermine Democracy", (2017) [last accessed 7 July 2022].
[121] Silverman, Craig & Kao, Jeff, "Infamous Russian Troll Farm Appears to be Source of Anti Ukraine Propaganda", *Talking Points Memo,* 11 March 2022 [last accessed 7 July 2022].
[122] https://www.nytimes.com/2022/03/11/opinion/russia-ukraine-cyberattacks.html

Microsoft[123] and other private actors[124] tell a very different story. There has been an abundance of cyberattacks, including on critical infrastructure installations. Furthermore, there seems to be coordination between cyberattacks and conventional kinetic attacks, providing examples of "hybrid warfare". Private companies have contributed ICT security services and ICT infrastructure and are playing a material role in the course of the conflict. Finally, information has been instrumentalized and "weaponized" in ways that are influencing the outcome of the war. Taken together, these elements offer food for thought about the future of warfare, and the existing normative and regulatory frameworks that govern it.

*Hybrid (Cyber) Warfare: Case Study on Microsoft's Activities in the Ukraine War*

The notion of "hybrid warfare" is increasingly finding purchase in articles and military documents, particularly with the increase of non-state actors and ICTs being deployed within the battlespace. While there is no universally-agreed (legal) definition for the term, and in fact use of the term has been criticized for lacking conceptual clarity[125], NATO describes "hybrid warfare" as entailing an "interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion. These instruments or tools are blended in a synchronized manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects."[126]

The interplay of both conventional and unconventional "instruments of power and tools of subversion" have certainly been visible on the conflict in Ukraine, which Microsoft's "Special Report: Ukraine, An overview of Russia's cyberattack activity in Ukraine"[127] (Microsoft Report I) and Microsoft's "defending Ukraine: Early Lessons from the Cyber War" (Microsoft Report II)[128] document. Even before the invasion, Microsoft found signs that Russia-aligned threat groups[129] were "pre-positioning for conflict"[130] as early in March 2021 with increased cyber incidents against Ukrainian and other organizations allied with them. These included phishing

[123] Burt, Tom, "Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine", 27 April 2022 [last accessed 7 July 2022].

[124] Cyber Peace Institute, *Ukraine: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects* [last accessed 7 July 2022].

[125] Reichborn-Kjennerud, Erik & Cullen, Patrick, "What is Hybrid Warfare?", Norwegian Institute of International Affairs (1/2016) [last accessed 7 July 2022].

[126] Bilal, Arsalan, "Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote," published 30 November 2021 [last accessed 7 July 2022].

[127] Burt, Microsoft Report I

[128] Smith, Brad, *Defending Ukraine: Early Lessons from the Cyber War*, Microsoft, 22 June 2022 [last accessed 7 July 2022].

[129] For more information about these kinds of groups, see Buzatu, Anne-Marie, "Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace", *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press, 21 April 2022.

[130] Burt, Microsoft Report I, p. 5.

campaigns[131], exploiting vulnerabilities in unpatched[132] Microsoft Exchange servers, compromising other IT service providers in the supply chain, and infiltrating the networks of Ukrainian energy and IT providers. In January 2022, after diplomatic efforts failed to deescalate tensions, Microsoft's Threat Intelligence Center (MSTIC) found wiper malware[133] in more than a dozen networks in Ukraine, subsequently alerting the Ukrainian government and publishing the findings.[134] Taken together, these activities "appeared aimed at securing persistent access for strategic and battlefield intelligence collection or to facilitate future destructive attacks in Ukraine during military conflict."

Of particular interest, the Microsoft Report I has two timelines that convey the hybridity of Russian-affiliated attacks. The first is a timeline of Political-military attacks juxtaposed against cyberattacks. It demonstrates how political events driving increased tensions such as meetings between Russian and Ukrainian officials coincide with cyberattacks, which were launched within a day or two, culminating in a cyberattack of wiper software against 19 Ukrainian government and critical infrastructure entities launched on 23 February 2022[135], the day before the physical invasion the Russian physical invasion of Ukraine. This was subsequently accompanied by a DDoS attack on Viasat, disrupting broadband internet services to large numbers of Ukranians as well as throughout Europe.

In similar fashion, the second timeline shows military attacks vis-à-vis cyberattacks. In many cases a cyberattack precedes a related kinetic attack, such as the March 4 cyberattack on the network of Vinnytsia followed by a March 6 launch of eight missiles at Vinnytsia. According to the report, "[a]nalysis of Microsoft signals … shows high concentrations of malicious network activity frequently overlapped with high-intensity fighting during the first six plus weeks of the invasion."[136] Toward the end of the report, Microsoft indicates that it has provided "real-time threat intelligence and guidance" to help Ukrainian's efforts to identify and counter cyberattacks, also saying that it has partnered with cyber threat intelligence company RiskIQ to provide "actional information" about unpatched Ukrainian government systems that would be more vulnerable to attack. Furthermore, it indicates that "with the consent and cooperation of the Ukranian government", it has helped to "proactively update systems with cyber countermeasures" and provided other technical guidance and assistance measures to increase ICT security.

[131] A phishing campaign uses emails disguised as coming from a trustworthy sender to try to obtain information such as login details or credit card information.

[132] This refers to ICT software where vulnerabilities have been found, but haven't been remedied, or "patched" with updates. Unpatched ICT systems are a major vector allowing cyber-attacks to propagate.

[133] Wiper malware erases the data on ICT systems.

[134] Microsoft Security, "Destructive malware targeting Ukranian organizations", 15 January 2022 [last accessed 27 July 2022].

[135] Microsoft Report II, p. 8.

[136] Burt, p. 10

In its second report published in June 2022, Microsoft reported that Russia's cyberattacks have not been limited to targets in Ukraine but have been aimed outside of Ukraine's borders. MSTIC has detected Russian cyberattacks against 128 targets located in 42 other countries, representing "a range of strategic espionage targets likely to be involved in direct or indirect support of Ukraine's defense." 49% of these attacks are identified as government agencies, 12% on NGOs that have been providing some kind of humanitarian or logistical support to Ukraine defense efforts, while the remaining 39% have been against commercial actors, including ICT, energy, critical defense companies.[137]

Finally, Microsoft says it has informed the US government about its activities and established communication channels with NATO and other EU cyber officials to inform them about attacks that have threat impacts outside of Ukraine.[138] Its extensive cybersecurity support to the Ukraine government, which Microsoft says has amounted to $239 million in financial and technology assistance at no charge to Ukraine as of June 2022, demonstrates the "role the private sector now plays in protecting a country in a time of war."[139]

While at the time of writing it is difficult to predict how cyber "hybrid warfare" of the Ukraine conflict will change future battlespaces, current trends indicate that cyber operations and the role of the private sector will feature prominently. Furthermore, cyberoperations in time of armed conflict carried out by actors—both state and non-state—located in other jurisdictions that the warring countries raise the oft-posed question of what kind of cyberattack meets the threshold of an armed attack, as well as how must a state (or potentially its important private actors) "cyber behave" to remain neutral within an armed conflict. While state behavior seems to indicate that there is a different threshold for cyberattacks to crystalize into a use of force or armed attack within the meaning of IHL, at the time of writing it is still not clear what "scale and effects" of cyberattacks would reach this threshold.[140]

*Case Study: Starlink Supporting communications and energy infrastructure*

On February 26, two days after the Russian invasion and simultaneous cyber attack on internet broadband service, Ukranian Vice President Mykhailo Fedorov tweeted on Elon Musk's account:

[137] Microsoft Report II, p. 11.

[138] Burt, p. 16

[139] Microsoft Report II, p. 10.

[140] The "scale and effects" test was first articulated in ICJ's 1986 Nicaragua v. United States case and repeated in the Tallinn Manual to determine when a cyber-attack would amount to a use of force or armed attack as articulated in the Geneva Conventions. Examples of cyber operations which may amount to a use of force include those that result in injury or death to persons, those that compromise military defense systems, or that cause serious financial, economic damages. However, despite expressions of opinion and military doctrine, in practice states have been reluctant to equate actual cyberattacks as uses of force or armed attacks, even when they resulted in serious injury or loss of life.

> *@elonmusk, while you try to colonize Mars—Russia try to occupy Ukraine! While your rockets successfully land from space, Russian rockets attack Ukranian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand.*

Thirteen hours later, Elon Musk tweeted back:

> **Starlink** service is now active in **Ukraine**. More terminals en route.[141]

Two days later, on February 28, Fedorov posted a picture of him unboxing a Starlink modem.[142]

As of the time of this writing, Starlink has shipped over 12'000 satellite modems to Ukraine, and Vice President Federov has said that "all critical infrastructure uses Starlink, all structures that are needed for the state's functioning use them." He went on to highlight the importance of the modems for the war effort, "they are one of the elements of the foundation of our fight and resilience." [143]

*Case study: Repurposing civilian ICT services for wartime purposes*

An interesting development in the Ukraine war is how the Ukrainian government has repurposed civilian apps for peacetime purposes. In February 2020, President Zelenski launched an e-government app called "Diia", in which he said that Ukrainians would soon have "the whole country in their smartphone".[144] The app stores people's identity cards, passports, drivers license, allows them to pay taxes and provides other government services. However, after the Russian invasion, the app added a new service. After only a simple update, the app contained a new feature called "E-Enemy", which allows Ukrainian citizens to provide information on Russian troop movements. Users have to login and authenticate themselves using the e-passport system. This is to provide assurances that the information is sent by a Ukranian person, and not by a Russian bot.[145]

Another civilian website, bachu.info, has also been transformed to support and direct Ukraine armed forces members fighting on the ground. Previously used as a site to report instances of minor infractions (e.g., neighbor not disposing of trash properly) it now has been updated

[141] https://twitter.com/MarcCieslak/status/1497760047870496773?s=20&t=Hkts8g5ttTTjA91r_oechw

[142] https://twitter.com/michaeldweiss/status/1498430369540063234?s=20&t=Hkts8g5ttTTjA91r_oechw

[143] Dudik, Andrea and Rosalind, Mathieson, "Ukraine Urges Musk's Starlink to Keep Helping Alongside Weapons", Bloomberg, 23 May 2022 [last accessed 27 July 2022].

[144] Trubetskoy, Denis, "Ukraine digital: Der Staat in einer App", MDR.de, 20 February 2020 [last accessed 27 July 2022].

[145] Artashyan, Argam, "Ukraine uses app DIIA to find Wherabouts of Russian Troops", Bizchina, 19 April 2022 [last accessed 27 July 2022].

to receive pictures and other information of Russian troop movements and uses AI to analyze them so that visual markings, units, equipment, etc. can be identified, The findings are then reviewed by a human at Ukrainian government security services, and then if approved are broadcast on the Bachu app.

*Case study: Use of Clearview AI in Ukraine*

Clearview AI is an American facial recognition company that provides services to law enforcement agencies and companies.[146] It has amassed a database of over 10 billion images,[147] that it has drawn from multiple sources, including social media platforms,[148] and more than 2 billion images from the Russian social media service VKontakte.[149] It is considered by many to provide the most reliable facial recognition services, claiming a better than 99% recognition accuracy "across all groups, regardless of age, gender, ethnic background, or race".[150] Having operated below the radar for several years, it came to widespread attention when the *New York Times* published an exposé on its services in January 2020[151], sparking outrage among civil liberties organizations and leading to several law suits being filed,[152] as well as several European Countries banning or restricting its use.[153]

After the Russian invasion of Ukraine, Clearview's CEO Hoan Ton-That offered its services to Ukraine, who initially rejected it, but then had a change of heart.[154] While there haven't been official reports on how Ukraine has been using the technology, numerous reports have made educated guesses and inferences. These include: to identify Russian casualties and prisoners of war; to undermine propaganda by, for example, debunking Russian claims that videos showing their troops committing war crimes are in fact fakes staged by the Ukrainians as their technology can identify the names and nationalities, and to identify Russians masquerading as Ukrainian forces, which has been reported by Ukrainian officials on Twitter.[155]

[146] In May 2022, Clearview AI agreed to a permanent injunction on selling access to its photograph database to companies in the US as part of a settlement to a lawsuit filed by the ACLU. , last accessed 29 May 2022.
[147] Clearview AI Principles [last accessed 19 May 2022].
[148] Lockett, Will, "The AI Defending Ukraine", *Medium,* 2 June 2022 [last accessed 7 July 2022].
[149] Dave, Paresh and Dastin, Jeffrey, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war", Reuters, 14 March 2022 [last accessed 7 July 2022].
[150] Clearview AI Principles.
[151] Hill, Kashmir "The Secretive Company That Might End Privacy as We Know It". *The New York Times*, 18 January 2020*, ISSN 0362-4331,* [last accessed 22 May 2022].
[152] Stubbs, Molly, "Clearview AI Faces Fourth Lawsuit Alleging Biometric Privacy Violations", Expert Institute, 25 June 2020 [last accessed 7 July 2022].
[153] EDRi, "About Clearview AI's mockery of human rights, those fighting it, and the need for the EU to intervene" 6 April 2022 [last accessed 7 July 2022].
[154] Lockett, Will.
[155] https://twitter.com/visegrad24/status/1497311883455610886?s=20&t=51JA76sdMVBFd_4r7v2X9Q
Dressing up in the uniform during an armed conflict is a clear violation of Article 39 of Additional Protocol 1 to the Geneva Convention. Russia withdrew from the Additional Protocol in 2019.

The conflict in Ukraine demonstrates that ICTs are being used by both state and non-state actors to facilitate and support armed attacks, as well as a number of other important manners, including using mis/disinformation to destabilize societies and influence morale. The extent to which these cyber incidents are changing the character of armed conflict, as well as the degree to which existing relevant international regulatory frameworks such as the Geneva Conventions and the Rome Statute of the International Criminal Court are able to effectively respond to these developments, is an area worth of further study and consideration.

*PSCs in Ukraine*

As a final note, at the time of this writing there have been numerous reports of the traditional "boots on the ground" PSCs being hired by governments to support operations in Ukraine. Undoubtedly, these actors are using many of the technologies described above in providing these services. However, as of now little has been reported on this angle, therefore mapping this angle of the private security sector will require additional work and time not originally foreseen in the scope of this mapping study. However, the author considers this an important topic to research more thoroughly.

**Bringing it all together through a human rights lens**

I. The Surveillance Society

The foregoing pages identify, and map increasing uses of ICTs by companies to gather and collect information about persons, institutions and governments, as well as weaponization of and attacks on information to destabilize societies. While each of these instances can raise alarms about invasion of privacy and other human rights impacts, taken together the widespread capture, analysis and synthesis of datapoints can create a widespread surveillance network with chilling effects on our exercise of freedoms and human rights.

*China's ICT-enabled surveillance state*

The *New York Times* published a report in June 2022 detailing how the Chinese government is constructing a "surveillance state" using many of the technologies that were described above in the mapping. Analyzing over 100,000 government bidding documents, it found the government had solicited bids from contractors for technologies and services to keep its citizens under constant surveillance. The ICTs included phone trackers, equipment to collect iris scans and sophisticated video cameras equipped with facial recognition and other technologies. Analysts estimate that half of the world's one billion video cameras are located in China. Documents obtained by the *Times* indicated that authorities are aiming for "maximum surveillance" such that their devices are placed in areas where people shop, live, go to school or work, or otherwise "fulfill their most common needs." Phone trackers are used to connect persons' digital lives to their physical locations. and connect with physical WIFI points located on the streets equipped with IMSI catchers and WIFI sniffers. These devices capture unique identification information on phones and monitor the information people input to apps, such as posts make on social media platforms.

These multiple data points are captured and analyzed by software platforms such as the one offered from Megvii, one of China's biggest surveillance contractors. Megvii's technology brings together many different types of personal data from mobile phones, video surveillance cameras and other sources, and "can display a person's movements, clothing, vehicles, mobile device information and social connections." The report goes on to describe a new effort to systematically collect biometric data, including voice prints, iris scans and even DNA samples of individuals, with Chinese authorities saying that this information is primarily used to track criminals. However, this assertion is belied by the documents that indicate this information is being collected in some provinces in an indiscriminate manner that does not distinguish between criminals and the general population.

For example in the city of Zhongshan, microphones are distributed along with video cameras to record audio within a 100-meter radius to analyze conversations with voice recognition software and collect the voiceprints into a database. Another document reveals that in Xinjiang, home to millions of Uyghurs, a contractor has built a database that can hold iris scans of up to 30 million individuals, and this same contractor is now building databases across other areas of the country. According to the *Times,* the Chinese government is capturing and consolidating all of these data points with the overarching goal of building "a comprehensive profile for each citizen" and using mass surveillance to support authoritarian rule.[156]

A subsequent article by the *New York Times* reported on a large-scale data breach of a Chinese government system, with an unknown hacker offering terabytes of data on a billion Chinese for sale for 10 Bitcoin, or about $200,000. Samples of the data reviewed by the *Times* included extremely personal information, including private information about political dissidents. The article also reported on the abuse of a Covid app by Chinese authorities to flag persons in volved in protests; the persons were erroneously flagged as being Covid positive, which prevented their free movement.

While this portrait does describe a state-controlled mass surveillance system, according to the documents the technologies and support services to deploy them are provided by private commercial actors. It also illustrates the degree to which the datapoints taken from different ICTs can be woven together using sophisticated software to invade privacy on a grand scale as well as to identify and follow persons of interest—in a similar fashion to the way in which Big Data Analysis services are processing and selling information on the marketplace.

*Surveillance advertising*

[156] Cardia, Alexander, Mozur, Paul and Xiao, Muyi, "China's Surveillance State is Growing. These Documents Reveal How", *New York Times,* 21 June 2022 [last accessed 27 July 2022].

China's use of ICTs to monitor its citizens is one example of highly regulated and coordinated synthesis of data points to control its citizens and may seem far for those living in places where technologies are not wielded so heavily by the state. Nevertheless, another actor has become adept at collecting, analyzing and synthesizing many of these same kinds of data points, and this is the advertising industry. While the surveillance advertising sector is largely beyond the scope of this study, the kinds of information obtained and the personal profiles created, are very similar to the practices described in the previous section on China; the main difference is that this information is captured in order to influence consumers and their purchasing choices. Notwithstanding this difference, collection of this information can have important impacts on human security. As mentioned above, information collected by advertising in mobile phone apps is being bought and used by law enforcement officials to monitor and even arrest individuals. Along similar lines, this location information could be included in OSINT services provided by private commercial actors to track individuals.

## II. Cross-cutting issues

### *Accumulation and security of stored data*

As the preceding sections illustrate, in today's information society, we are generating enormous amounts of personal data, which are captured and stored on ICT systems all around the world without our necessarily knowing where it is located or who has access. Companies providing security services could be said to be capturing particularly sensitive information, whether it is from video surveillance, access control systems, drones or open source or proprietary datasets, which can be used to invade our privacy, follow our movements or surveil our interactions and behaviour.

### *Requests for personal information from governments and other actors*

A related point is government requests for access personal information that companies have stored on their systems. These requests can be indiscriminate or overbroad, and companies need to educate themselves about legal protections and what exactly is and is not allowed under applicable law to be able to respond with the least amount of personal/sensitive data as possible. Another finding which merits further attention is how companies share or sell data with other actors, including companies, as well as selling it as part of intelligence services to public *and* private actors, including big data analytics services. This mapping has brought into evidence the power and responsibility of companies to protect human rights through their management and safeguarding of sensitive information they collect through their services, and by exercising due diligence of the clients they work with.

### *Vulnerable populations*

Vulnerable populations, such as women, non-binary persons, minorities and those with disabilities have higher risks of being attacked online, such as by cyber-bullying and cyber-stalking, and are frequently targeted by the "weaponization of information". The amounts of sensitive information collected in service of security services can be used to identify and target vulnerable populations, both online and offline. For example, Human Rights Watch has reported on the use of "weaponized surveillance technologies" by both China and Israel to suppress the peaceful dissent by Uyghurs and Palestinians.[157] This was also raised by human rights advocates and vocal critics of government practices, who have experienced being targeted by public and private security personnel for their advocacy practices, and who fear that online personal information can be used in tactics aiming to intimidate and silence them.

*The importance of reporting vulnerabilities*

As illustrated in the discussions above, one of the biggest (human) security threats is the exploitation of vulnerabilities in ICT systems. However, companies can be reluctant to report vulnerabilities in their systems for a number of reasons, including fear that the vulnerabilities will be further exploited by other actors before they are patched or secured, as well as reputational damage and fear of loss of business. While there are some valid reasons to delay public notification of discovery of vulnerabilities, it is important that they are reported as soon as is responsibly possible in order to notify affected customers and users of the compromise of their data, as well as to inform others who may be affected by the same vulnerability so that they can take measures to safeguard their systems.

## III. Setting Standards

Based on the foregoing discussions, it is recommended that the following policies and practices are developed for and implemented by companies providing security services utilizing ICTs:

*Good Practices*

- *Collect less rather than more:* in providing security services, companies should endeavour to collect the least amount of data possible to carry out their business practices in a responsible manner;
- *Time limits on storing information*: Information that is collected should be stored on company systems for limited times and then discarded responsibly;
- *Transparency:* companies should inform their clients in an easy-to-understand manner of the types and kinds of information they collect, as well as how long they have such information saved on their systems. Importantly, they should also provide users and those subject to having their personal information collected with possibilities to opt-out of this data collection;
- *Adopt robust information security practices*: Companies should implement robust information security practices and procedures that are in line with the highest industry

[157] Shakir, Omar, "Mass Surveillance Fuels Oppression of Uyghurs and Palestinians", Human Rights Watch, 24 November 2021 [last accessed 27 July 2022].

standards, as well as develop human-rights compliant responses in the eventuality that their systems are breached and sensitive information is accessed by malicious actors. For example, end-to-end security means that all information is encrypted on the companies' systems, so that even if it is breached, it cannot be read by the attackers;

- *Capacity building:* Companies need to train their personnel on human-rights compliant practices and procedures for capturing, storing, accessing, managing and deleting information they obtain within the provision of their services, both information obtained from clients, as well as information about third persons, places, communications, and any other data exchanges and transactions.

Due Diligence

- Selecting Clients*:* One of a company's greatest abilities to protect human rights is through the selection of its clients. Carrying out a robust due diligence exercise before engaging with clients and using that as a decisive indicator in deciding whether or not to do business with a client (either non-state or state) helps to reduce human rights injuries and violations, even in countries with poor human rights records. The GNI has developed "open source" procedures that can be adapted to businesses who are not part of the initiative.
- *Sharing information with government authorities*: Similarly, adopting robust policies and procedures for how to respond to government responses for personal data and information is another tool companies have to help reduce human rights violations.

Transparency

- Vulnerability sharing: Companies should implement responsible procedures for sharing vulnerabilities that minimize human rights risks of those whose data could be potentially compromised as well as to reduce the likelihood that other computers will be similarly affected. The European Union Agency for Cybersecurity (ENISA) published a good practice guide on vulnerability disclosure in 2016.[158]
- *Explainability:* Companies developing and using AI should whenever possible use "Explainable AI" (XAI), or "Explainable Machine Learning" (XML) which provides computing processes and results that and explainable to humans,[159]

Accountability and access to remedy

Companies should hold themselves to account for respecting these principles and good practices and provide effective remedies to those who are injured by their activities.

[158] See, e.g., Enisa, "Good Practice Guide on Vulnerability Disclosure. From Challenges to recommendations" (2016) [last accessed 27 July 2022].
[159] An example of the use of XAI and XML can be found here: https://www.mdpi.com/1999-4893/15/2/49 [last accessed 27 July 2022].

Initiatives such as OHCHR's Guiding Principles on Business and Human Rights and B-Tech initiatives, as well as the ICoC/A provide relevant guidance and examples for non-state company-based grievance mechanisms.

**Looking forward: recommendations and next steps**

This mapping study does not aim to be proscriptive and provide canned solutions to the above challenges. Rather, it aims to start and add to discussions about how current and evolving ICTs in security services provided by commercial actors can be deployed responsibly and in a manner that respects while human rights. To that end, the author makes the following recommendations:

*Identify gaps in existing relevant norms and regulatory frameworks*

- Carry out a detailed gap analysis of relevant oversight, accountability and governance frameworks, including but not limited to the ICoC/A, Montreux Document, Wassenaar Arrangement, and Voluntary Principles on Security and Human Rights.
- Identify good practices and lessons learned from other initiatives, including the Guiding Principles on Business and Human Rights/ B-Tech and the Global Network Initiative.

*Update existing regulatory frameworks*

Carrying out a gap analysis as well as identifying good practices from other initiatives sets the stage for processes to "translate" those good practices into formats that are adapted to security services utilizing ICTs, and which respond to the particular human rights sensitivities inherent to those services. Developing robust due diligence standards for the use of ICTs in the provision of security services by private actors would be particularly effective in reducing/preventing violations of human rights. The ICoC and its multistakeholder oversight and governance process would provide a good framework to update in order to incorporate human-rights protecting principles and standards for security services utilizing ICTS.

*Coordinate it through a multistakeholder platform*

The overview of governance initiatives in Section II provides some guidance for the kinds of characteristics such a platform should have. As a first matter, the notion the ICTs are now an integral part of private security services should be explicitly recognized, as has been done in the South African study. Robust due diligence procedures and the responsibility of the company to ensure that its services are not used to violate human rights is another important element that has been recognized by GNI and the UNGPs/B-Tech initiatives. Multistakeholder governance processes which recognize the particular areas of "effective control" that each stakeholder group brings to the table are another essential element for filling governance gaps and establishing effective oversight of and accountability for human rights violations. Finally, the conflict in Ukraine illustrates how closely ICTs are entwined with military operations. The Montreux Document process could provide a model or could provide a platform for further discussions about how to use ICTs in security services provided within the context of an armed conflict in line with IHL obligations. Finally, the situation of armed conflict casts both ICT4Peace's 2011 call for a Code of Conduct for Cyberconflicts[160] and Microsoft's Geneva Digital Convention in a different light, and this could provide some guidance for how states should utilize ICTs when at war.

The current proposal for a UN Programme of Action could provide a venue from which these activities could be coordinated. Care should be taken to ensure that appropriate non-state actors, including representatives from pertinent companies, civil society organizations, ICT experts, and academics are included in a meaningful fashion in order help ensure effective results. Coordinating it through a UN body in which can act as a kind of "hub" into which the plethora of existing initiatives can feed into also could help to reduce the complexity and subject-matter overlap/misalignment of the plethora of initiatives that are working on relevant initiatives, and allow then to contribute more efficiently and effectively within the areas where they have experience and subject-matter expertise.

However, mindful that some states are very resistant to non-state actor participation, it may be more pragmatic to carry out this work outside of, but with close ties to, the UN. Another approach could be to form an alliance among existing multistakeholder groups and initiatives that have expertise, resources and convening power to carry out the above steps. Along these lines, here follow some proposals:

- Organize meetings within the Montreux Document Forum to discuss the increasing use of ICTs in the provision of private military and security services within the context of an armed conflict;
- Drawing upon the resources of International Geneva, Switzerland could convene a working group on updating standards for ICTs used in security services by companies, supported by the ICoCA providing expertise in the private security industry, and led by ICT4Peace Foundation as subject-matter experts with experience in both ICTs as well as private security services. Its findings could then be used to inform and update relevant regulatory frameworks, including the ICoC, and Swiss import-export standards.

[160] Stauffacher, Daniel Sibilia Ricardo Weekes Barbara, Getting down to business: Realistic goals for the promotion of peace in cyberspace ICT4Peace Foundation (2011) [last accessed 7 July 2022]. See also Stauffacher Daniel, Drake William, Currion Paul, Steinberger Julia, Information and Communication Technology for Peace - The Role of ICT in Preventing, Responding to and Recovering from Conflict ,
The United Nations Information and Communication Technologies Task Force, New York (2005) [last accessed 7 July 2022].

- Develop capacity-building courses for ICoCA Member Companies on how to responsibly use ICTs in their provision of private security services. ICT4Peace Academy in cooperation with ICoCA could jointly develop these courses.

*Develop effective oversight and remedial processes*

Initiatives such as the Guiding Principles, B-Tech and ICoCA offer examples for developing processes to provide effective remedies in the event of human rights injuries and violations, as well as governance frameworks to prevent those injuries and violations. Particularly interesting are the examples where company remedial processes are required by either national law / national procurement policies, or within the service contract (whether with a private or public client). These measures supporting accountability can have the effect of "hardening" soft law and deliver monetary or other important sanctions that can motivate a company to take the necessary steps to prevent negative impacts on human rights. Including such measures in contracts avoids difficulties inherent in extraterritorial application of national law, and therefore can help to fill in some of these governance gaps.[161]

*Develop capacity-building for relevant companies*

As mentioned previously, numerous traditional PSCs are now offering ICT-related or enabled services without receiving training on how to best protect human rights. Capacity-building courses that provide guidance and good practices on how to responsibly use ICTs in their services can help to reduce/minimize human rights abuses.

**Conclusion**

As a final note, the author would like to highlight that the findings of the mapping study raised more human rights concerns than originally expected, reflecting both the journey of the study as well as the evolution of the understanding of what makes us secure. Information collection, storage and analysis have always been an integral part of security provision, but what has changed in recent years is the vast amount of information data points that are available for this collection, as well as the sheer numbers of persons who participate in this information ecosystem, often sharing deeply personal and sensitive information about themselves. This coupled with the ways in which this information can be used to mislead, threaten or coerce can undermine the principles and values that underly democratic societies. It is hoped that this study raises more awareness about how ICTs are being used, and the associated human rights and societal impacts, so that our legal and governance frameworks can be updated in such a manner to mitigate their negative impacts and realize the enormous potentials of ICTs for good.

[161] For more in-depth discussion on this topic, see Buzatu DCAF SSR Paper 12

## Annex I: List of Interviewees

1. **Jelena Aparac**, Member of Working Group on the use of Mercenaries
2. **Assesandro Arduino**, Principal Research Fellow, Middle East Institute, National University of Singapore
3. **Marie McAuliffe**, Head of Migration Research Division and Editor of the World Migration Report at the International Organization for Migration
4. **Beril Atuk**, Channel Account Manager of B!nalyze Digital Forensics
5. **Maria Baratta**, Project Manager at Trygg
6. **Doug Brooks**, Vice President at FGi Solutions
7. **Andrew Clapham**, Professor of International Law, Graduate Institute of International and Development Studies
8. **Laura Crespo**, Deputy Head, Office for Cyber Foreign and Security Policy, Swiss Federal Department of Foreign Affairs
9. **Sorcha McCloud**, Associate Professor/Marie Curie Fellow/Chair of the UN Working Group on the use of Mercenaries
10. **Gary Corn,** Director, Technology, Law and Security and Adjunct Professor of Cyber and National Security Law
11. **Darla Davitti**, Senior Lecturer, Associate professor, Senior lecturer, Department of Law, University of Lund
12. **Mark DeWitt**, Chief Legal Officer, GardaWorld Federal Services
13. **Jon Drimmer**, Partner at Paul Hastings, LLP, Strategic Adviser to the Volutary Principles on Security and Human Rights Initiative
14. **Serge Droz**, Board Member Forum of Incident Response and Security Teams (FIRST)
15. **Sam W. Evans**, Senior Research Fellow at the Program on Science, Technology & Society, Harvard University
16. **Alyson K. Finley**, Technology and Human Rights Analyst (contractor) at the US Department of State
17. **Martina Gasser,** Head of Export Control and Private Security Service Division, Swiss Federal Department of Foreign Affairs
18. **Alexandra Gerst**, Corporate Counsel, Microsoft Digital Crimes Unit
19. **Sabelo Gumedze**, Senior Researcher at Institute for Security Studies in South Africa
20. **David Jenkins**, Principal Health, Safety & Environment at BHP Billiton
21. **David Kaye**, Professor of Law at University of California at Irvine, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2014-2020)
22. **Mike Kelly**, President Palantir Technologies Australia
23. **Jerry Kloski**, Director Health, Safety, Security & Environment at Total
24. **Anna Leander**, Professor, International Relations/Political Science, Geneva Graduate Institute
25. **Charlie Mayne**, CEO VSC Security Solutions
26. **Dylan Muir**, VP Global Research Operations at SynSense, Data Cross
27. **Jason Pielemeier**, Executive Director at the Global Network Initiative
28. **Tilman Rodenhauser**, Legal Adviser at the International Committee of the Red Cross (ICRC)

29. **Monika Ruiz**, Program Manager/ Digital Diplomacy Strategist at Microsoft
30. **Florian Schuetz,** Federal Cyber Security Delegate at Swiss FDFA
31. **Jai Shah**, Cybersecurity contractor of Archer International
32. **Jenny Stein**, Special Advisor for Internet Freedom and Business and Human Rights at US Department of State
33. **Severin Trösch**, Senior Data Scientist at Datahouse AG, member of DataCross network
34. **Mauro Vignati**, Adviser Digital Technologies of Warfare at the International Committee of the Red Cross (ICRC)
35. **Sylvia White**, Director, Risk, Legal and Compliance, Osprey Flight Solutions
36. **Hloniphani Xulu,** researcher at South African Private Security Industry Regulation Authority.

## Annex II: Quantitative research on companies using ICTs in the provision of security services

In carrying out the research for this mapping study, the author endeavoured to get a sense of the numbers of companies providing the services that are identified in this study. Partnering with Datacross, a non-profit Swiss association staffed entirely by volunteer data scientists who donate their time free of charge to NGOs to support their work.

Datacross carried keyword searches of the LinkedIn database using search terms derived from the initial findings of the mapping study.[162]

The search term queries returned a little more than **10'000** companies worldwide providing security services using ICTs. While LinkedIn is not a comprehensive listing of all companies globally, these results do give a sense of the magnitude of the sector.

Datacross also carried out queries of commercial registries in Switzerland and the United Kingdom. The query in Switzerland returned **884** companies. The query in the United Kingdom returned **505** companies.

Given the comparatively small size of Switzerland relative to the United Kingdom, the higher number of companies registered in Switzerland indicate that it is an important and growing host country for companies providing ICT-enabled security services.

[162] Search Terms - Private Cyber Security Companies Project

Surveillance, Biometrics, Location tracking, Robots, Drones, Security Apps, Cyber threat assessments, Industrial control systems, Cyber-secured positioning, Cyber attack defense, Remote Monitoring, Facial recognition, location metadata, robot perimeter guarding, drone surveillance, Security apps using GPS,Advance Persistent Threats (APT),critical infrastructure,cyber-secured navigation,Identifidation of cyberattack authors,Video surveillance, Iris scans, biometrics, GPS tracking, armed robots, armed drones ,Data collection app, Ransomware,energy grid security,cyber-secured timing,Honeypots,Metadata surveillance, Fingerprint biometrics, Location tracking App, robots AI drones, AISecurity camera app, Maiware, water systems security, securing GPS, 5G/4G, wifi, IP blacklisting, Surveillance App, Biometric App, robots, detention services, drones convoy protection, Risk alert app, Supply chain vulnerabilities,banking systems security, digital dye packs, drones location tracking, cyber security, government systems security, traffic shaping/sinkholes, drones migration tracking, Hackbacks, white hat hacking, Web Intelligence Services, Dark Web Intelligence Services, Artificial Intelligence Services, Virtual Private Networks, VPN

## Annex III: References

Achiume, Tendayi, *Racial discrimination and emerging digital technologies: a human rights analysis – Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, 18 June 2020, A/HRC/44/57 [last accessed 7 July 2022].

Amnesty International, "Uncovering the Iceberg, the Digital Surveillance Wrought by States and the Private Sector", (2021) [last accessed 7 July 2022].

Baker, Steward, *The Flawed Claims about Bias in Facial Recognition*, Lawfare Institute, 2 February 2022 [last accessed 7 July 2022].

Bilal, Arsalan, "Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote," published 30 November 2021 [last accessed 7 July 2022].

Burt, Tom, "Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine", 27 April 2022 [last accessed 7 July 2022].

Buzatu, Anne-Marie, "Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace", *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press, 21 April 2022 [last accessed 27 July 2022].

Buzatu, Anne-Marie, *Towards an International Code of Conduct for Private Security Providers: A View from Inside a Multistakeholder Process*, DCAF SSR Paper 12 (2015) [last accessed 7 July 2022].

Cardia, Alexander, Mozur, Paul and Xiao, Muyi, "China's Surveillance State is Growing. These Documents Reveal How", *New York Times,* 21 June 2022 [last accessed 27 July 2022].

Clearview AI Principles [last accessed 19 May 2022].

Crawford, David and Fuhrmans, Vanessa, "Siemens Business Surges in Iran", *The Wall Street Journal*, 5 April 2011 [last accessed 7 July 2022].

Cyber Peace Institute, *Ukraine: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects* [last accessed 7 July 2022].

Dave, Paresh and Dastin, Jeffrey, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war", Reuters, 14 March 2022 [last accessed 7 July 2022].

DeMuro, Jonas, "Best access control systems of 2022", Techradar, 19 May 2022 [last accessed 7 July 2022].

Diab, Robert, "Compelling people to reveal their passwords is posing a challenge to police and courts", *The Conversation,* 22 May 2019 [last accessed 7 July 2022].

Dudik, Andrea and Rosalind, Mathieson, "Ukraine Urges Musk's Starlink to Keep Helping Alongside Weapons", Bloomberg, 23 May 2022 [last accessed 27 July 2022].

Duguin, Stéphane, "Renewed call for moritorium on sale and use of spyware", Cyber Peace Institute, 25 May 2022 [last accessed 7 July 2022].

EDRi, "About Clearview AI's mockery of human rights, those fighting it, and the need for the EU to intervene" 6 April 2022 [last accessed 7 July 2022].

European Parliament News, "EP inquiry committee for Pegasus and other spyware launched", 19 April 2022 [last accessed 27 July 2022].

Evans, Samuel, *Revising Export Control Lists*, Flemish Peace Institute, 24 March 2015 [last accessed 7 July 2022].

Finews.com, "Credit Suisse leans into Palantir", 15 November 2018 [last accessed 7 July 2022].

Fortinet, "What is ICS Security" [last accessed 27 July 2022].

*Freedom in the World 2022, The Global Expansion of Authoritarian Rule*, Freedom House (2022) [last accessed 7 July 2022].

*Manipulating Social Media to Undermine Democracy*, Freedom House, (2017) [last accessed 7 July 2022].

Gallager, Ryan, "Meta identifies 6 firms, including India's BellTrox, for "indiscriminate" surveillance", *The Print*, 17 December 2021 [last accessed 7 July 2022].

Géry, Aude, *Droit international et prolifération des cyberarmes*, « Politique Etrangère » 2018/2 [last accessed 7 July 2022].

*The GNI Principles,* Global Network Initiative (2008) [last accessed 7 July 2022].

Hill, Kashmir "The Secretive Company That Might End Privacy as We Know It". *The New York Times*, 18 January 2020, *ISSN 0362-4331*, [last accessed 22 May 2022].

Hvistendahl, Mara, "How the LAPD and Palantir use Data to Justify Racist Policing", *The Intercept,* 30 January 2021 [last accessed 7 July 2022].

*The International Code of Conduct for Private Security Service Providers*, ICoCA (2010) [last accessed 7 July 2022].

Jolly, Jasper, "Airbus to operate drones searching for migrants crossing the Mediterranean", *The Guardian,* 20 October 2020, [last accessed 7 July 2022].

Kaye, David, *Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 28 May 2019, A/HRC/41/35 last accessed 7 July 2022].

Kenyon, Miles, *The NSO Connection to Jamal Khashoggi*, CNN report published on YouTube, 22 October 2018 [last accessed 7 July 2022].

Korkmaz, Emre Eren, *Refugees are at risk from dystopian ¨smart border" technology*, 8 December 2020 [last accessed 7 July 2022].

Lockett, Will, "The AI Defending Ukraine", *Medium,* 2 June 2022 [last accessed 7 July 2022].

Lohrmann, Dan, *The Case for Establishing a Digital Geneva Convention Government Technology*, 8 August 2021 [last accessed 7 July 2022].

Microsoft Security, "Destructive malware targeting Ukranian organizations", 15 January 2022 [last accessed 27 July 2022].

Mijente, *Anduril's New Border Surveillance Contract with the US Marine Corps and CBP*, 24 July 2019, [last accessed 7 July 2022].

*The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*, (2008) [last accessed 7 July 2022].

National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022.

Nichols, Greg, *The 5 best surveillance drones: Next-level inspection UAVs, ZDNet,* 20 May 2022, [last accessed 27 July 2022].
Mazzeo, Antonio "Border surveillance, drones and militarization of the Mediterranean", *Statewatch,* 6 May 2021 [last accessed 7 July 2022].

*The 9 Principles*, Paris Call Initiative (2018) last accessed 7 July 2022].

*Overview of Existing Confidence Building Measures as Applied to Cyberspace*, GFCE, 03/06/20, *p.*7 [last accessed 7 July 2022].

Parascandola, Rocco and Moor, Tina, "Brooklyn rapper Bobby Shmurda arrested in gun, narcotics investigation", *Daily News,* 18 December 2014 [last accessed 7 July].

Pavone, Vincenzo, Jaquet-Chiffelle, *A systemic approach to security: Beyond the trade-off between security and liberty* , Taylor and Francis (2016) [last accessed 22 May 2022].

Pelroth, Nicole, *This is How They Tell Me the World Ends, The Cyber-Weapons Arms Race*, Bloomsbury Publishing, Kindle Edition (2021).

Penel, Charlotte and Petersohn, Ulrich, *Commercial Military Actors and Civilian Victimization in Africa, Middle East, Latin America and Asia 1980-2011*, Journal of Global Security Studies (2022=.

Perrigo, Billy, *Why Timnit Gebru Isn't Waiting for Big Tech to Fix AI's Problems*, *Time Magazine*, 18 January 2022 [last accessed 7 July 2022].

*Program of Action on the International Security Aspects of Information and Communication technologies and responsible State behavior in cyberspace* [last accessed 7 July 2022].

*Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 June 1977 [last accessed 7 July 2022].

*The Regulation of Foreign Military Assistance Act 15 of 1998* (FMA), The Republic of South Africa Government Gazette, 20 May 1998 [last accessed 7 July 2022].

Reichborn-Kjennerud, Erik & Cullen, Patrick, "What is Hybrid Warfare?", Norwegian Institute of International Affairs (1/2016) [last accessed 7 July 2022].

Ruan, Lotus, Knockel, Jeffrey and Crete-Nishihata, Masashi, *Censored Contagion, How Information on the Coronavirus is Managed on Chinese Social Media*, Citizenlab, 3 March 2020 [last accessed 7 July 2022].

*The Prohibition of Mercenary Activities and Regulation of Certain Activities in Country of Armed Conflict Act 27 of 2006* [last accessed 7 July 2022].

Savage, Charlie, "Intelligence Analysts use US Smartphone Location Data without Warrants, Memo Says", *New York Times*, 22 January 2021 [last accessed 7 July 2022].

Shakir, Omar, "Mass Surveillance Fuels Oppression of Uyghurs and Palestinians", Human Rights Watch, 24 November 2021 [last accessed 27 July 2022].

Sharma, Ax, Breeden II, John and Fruhlinger, Josh, "15 top open-source intelligence tools", CSO online, 28 June 2021 [last accessed 7 July 2022].

Silverman, Craig & Kao, Jeff, "Infamous Russian Troll Farm Appears to be Source of Anti Ukraine Propaganda", *Talking Points Memo,* 11 March 2022 [last accessed 7 July 2022].

Smith, Brad, *Defending Ukraine: Early Lessons from the Cyber War*, Microsoft, 22 June 2022 [last accessed 7 July 2022].

Smith, Brad.*The need for a Digital Geneva Convention*, 14 February 2017 [last accessed 7 July 2022].

Stauffacher, Daniel & Kavanagh, Camino, *Confidence Building measures and International Cyber Security*, ICT4Peace Foundation (2013), [last accessed 7 July 2022].

Stauffacher, Daniel  Sibilia Ricardo  Weekes Barbara,  Getting down to business: Realistic goals for the promotion of peace in cyberspace ICT4Peace Foundation (2011) [last accessed 7 July 2022].

Stauffacher Daniel, Drake William, Currion Paul, Steinberger  Julia, Information and Communication Technology for Peace - The Role of ICT in Preventing, Responding to and Recovering from Conflict ,The United Nations Information and Communication Technologies Task Force, New York (2005) [last accessed 7 July 2022].

Stubbs, Molly, "Clearview AI Faces Fourth Lawsuit Alleging Biometric Privacy Violations", Expert Institute, 25 June 2020 [last accessed 7 July 2022].

Summary of Report No. 74 regarding automated OSINT by the Dutch Committee on the Intelligence and Services", Dutch Review Committee on the Intelligence and Security Services, 08 February 2022, [last accessed 7 July 2022].

Trubetskoy, Denis, "Ukraine digital: Der Staat in einer App", MDR.de, 20 February 2020 [last accessed 27 July 2022].

Urbina, Ian, "Europe's border agency under fire for aiding Libya's brutal migrant detentions", NBC News, 29 November 2021 [last accessed 7 July 2022].

United Nations General Assembly (UNGA), *Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council*, 13 May 2011, A/HRC/WG.10/1/2 [last accessed 7 July 2022].

United Nations General Assembly (UNGA), *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security*, 10 March 2021, A/AC.290/2021/CRP.2 [last accessed 7 July 2022].

United Nations General Assembly (UNGA) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, A/70/174 [last accessed 7 July 2022].

United Nations General Assembly (UNGA), *Issue of human rights and transnational corporations and other business enterprises, report of the Working Group on the issue of human rights and transnational corporations and other business enterprises*, 21 July 2020, A/75/212 [last accessed 7 July 2022].

United Nations General Assembly (UNGA), *The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities - Report of the Working Group on the use of mercenaries*, 15 July 2021, A/76/151 [last accessed 7 July 2022].

United Nations Human Rights Council (HRC), *Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants*, 9 July 2020, A/HRC/45/9 [last accessed 7 July 2022].

*UN News,* "Moritorium call on surveillance technology to end 'free-for-all' abuses", 25 June 2019 [last accessed 7 July 2022].

*UN News,* "Spyware: Rights experts push for surveillance technology moratorium", 12 August 2021 [last accessed 7 July 2022].

United Nations Security Council (UNSC) "Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, UN, 8 March 2021 [last accessed 7 July 2022].

UpGuard, "Telecommunications Breakdown: How Russian Telco Infrastructure was Exposed", 18 September 2019 [last accessed 7 July 2022].

Ward, Jacob and Sottile, Chiara, *Inside Anduril, the startup that is building AI-powered military technology*, 3 October 2019, NBC News, [last accessed 7 July 2022].

Xulu, Hloniphani, *The new Private Security Industry: Regulating Cybersecurity Services* (2022) [not yet published].

Zetter, Kim, "Nokia-Siemens Spy Tools Aid Police Torture in Bahrain", *Wired Magazine,* 23 August 2011 [last accessed 27 July 2022].