**Submission to the Call for inputs: report on the provision of military and security cyber products and services by ‘cyber mercenaries’ and its human rights impact**

Noëlle van der Waag-Cowling1, Brett van Niekerk2 and Dr Trishana Ramluckan2,3

1Stellenbosch University, South Africa

2University of KwaZulu-Natal, South Africa

3Educor Holdings, South Africa

**Scope of the Document**

In view of the considerable range of global expertise in the UN OHCHR Working Group on Mercenaries, this submission will primarily focus on Africa and, by extension South Africa due to the location and fields of expertise of the contributing researchers.

Due to the unique nature of cyberspace, the submission begins by discussing the nature of cyber mercenaries and possible definitions and perspectives relate to this. This discussion will then inform the responses to specific items requested in the call for inputs.

The answers in this questionnaire will attempt to highlight and interpret this evolving and changing nature of mercenary activity through the cyber domain. For Africa, the growth of cyber mercenary activity poses two very specific threats to the continental peace and security architecture. Firstly, there are numerous ongoing conflicts, many of which involve multiple non-state and proxy actors and represent perfect platforms for hybrid warfare activities. Secondly, the massive increase in malicious cyber threats and actors leaves many states exposed. Capacitating less developed states to effectively defend against such threats is a long term, resource intensive project. This presents substantial opportunity and potential for PMSCs to augment and build cyber warfare capabilities in the region. The possibility that such operations can lead to either dependencies or begin to morph into mercenary types of activities will therefore be present.

**Defining Cyber Mercenaries**

Given the specific context of cyberspace, defining a ‘mercenary’ may be more complicated than for the traditional physical space. For instance, the concept of ‘patriotic hackers’ do not necessarily get paid as their activity could be purely ideological. This then deviates from the traditional definition of mercenary. A non-traditional, more contemporary term is ‘cyber proxy’, whereby this broader context can be encompassed. A defining and seminal work on this subject is Dr Tim Maurer’s book ‘Cyber Mercenaries: The State, Hackers and Power’ (2018).

The Tallinn Manual 2.0 (Schmitt, 2017) defines cyber-mercenaries along the lines of traditional mercenaries, in that they need to meet the following six criteria:

“special recruitment; direct participation in hostilities; desire for private gain as primary motivation; neither a national of a party to the conflict nor a resident of territory controlled by a party; not a member of the armed forces of a party to the conflict; and not sent by another State on official duty as a member of its armed forces.” (p. 412)

The implications of thiss is that cyber-mercenaries are considered unprivileged belligerents and are not considered as having combatant status. The Tallinn Manual also notes that civilians who participate in conflicts lost their protected status, and this extends to cyber space (Schmitt, 2017).

Article 1 of The International Convention against the Recruitment, Use, Financing and Training of Mercenaries (United Nations, 1989) defines mercenaries as:

“*1. A mercenary is any person who:*

*(a) Is specially recruited locally or abroad in order to fight in an armed conflict;*

*(b) 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 rank and functions in the armed forces of that party;*

*(c) Is neither a national of a party to the conflict nor a resident of territory controlled by a party to the conflict;*

*(d) Is not a member of the armed forces of a party to the conflict; and*

*(e) 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.*

*2. A mercenary is also any person who, in any other situation:*

*(a) Is specially recruited locally or abroad for the purpose of participating in a concerted act of violence aimed at :*

*(i) Overthrowing a Government or otherwise undermining the constitutional order of a State; or*

*(ii) Undermining the territorial integrity of a State;*

*(b) Is motivated to take part therein essentially by the desire for significant private gain and is prompted by the promise or payment of material compensation;*

*(c) Is neither a national nor a resident of the State against which such an act is directed;*

*(d) Has not been sent by a State on official duty; and*

*(e) Is not a member of the armed forces of the State on whose territory the act is undertaken.”*

The definitions used in the Tallinn Manual 2.0 and the International Convention against the Recruitment, Use, Financing and Training of Mercenaries follow that of a traditional mercenary. However, in the context and ambiguity of cyberspace, this definition may not be ideal. The structure of groups online are less formal than in the real-world, therefore individuals or groups could be involved in cyber mercenary activity without being fully aware of this. For example, the use of cyber-criminal infrastructure for circumventing attribution may also be a viable occurrence. In such instances, the cyber-criminals may not be aware of the end-use that their infrastructure (e.g. botnets) are being put to use; they may only see the IP address range to target for a DDoS, without understanding what is at the receiving end in the real-world. In addition, nations may leverage off volunteers or ‘patriotic hackers’ who are motivated by ideological reasons, and can perform actions in cyber space on behalf of a nation with minimal financial investment.

In 2019, the Foreign Minister of Rwanda, Richard Sezibera commented on Africa’s history of mercenaries, stating that they have “presented a grave threat to the independence, sovereignty, territorial integrity of Member States”. Importantly, Minister Sezibera drew attention to the changing nature of mercenary activity on the Continent and highlighted that the 1977 definition of mercenaries “may no longer be adequate to describe” today’s activities of the worrying increase of transboundary criminal networks…many connected to global terrorist networks”. “Today, mercenaries are not only involved in active combat, we now see an increase in cyber attacks and industrial espionage carried out by mercenary groups within the comfort of their own homes”, he said. As they continue to evolve and innovate, he argued: “We should not be static in our response” but update existing legal instruments to meet the unfolding challenges” (UN News, 2019).

The first question in the call for submission indicates beneficiaries can include both state and non-state actors; this implies a recognition that the traditional definition of cyber mercenaries does not hold in cyberspace, and this submission take this into account.

**Current trends and developments**

1. **Who are the clients and/or beneficiaries of cyber-capabilities and operations?***Clients and beneficiaries can include for instance both State and non-State actors who contract “cyber mercenaries” and other actors operating alone or through private military and security companies (PMSCs) to acquire cyber-capabilities, including military and security services and products.*

Given the ambiguity of the definition of a cyber mercenary as discussed above, there is a broad range of possible beneficiaries, including:

* States (or Territory/Regional Governments)
* Political Parties/Organisations/Movements
* Insurgent and Separatist Groups
* Terrorist Groups
* Criminal Syndicates (including Pirates)
* Commercial Consortiums/Individuals which are disposed to corrupt practices/IP theft or reliant on political connections
* Private Investigator entities (in particular those with underworld linkages)
* Human and Wildlife Trafficking Groups (including Poaching Syndicates)
* Assassins
* Warlords and their Militias
1. **What is the role of actors, operating alone or through PMSCs, in a) developing, b) maintaining, c) selling, d) delivering cyber-capabilities (incl. military or security products or services in cyber space) to third parties, or e) carrying out cyber espionage?**

A key challenge in this area is understanding the key differences between ‘traditional PMSCs’ and the rise of companies and consultants which ply their trade within the cyber mercenary domain. Many existing PMCs do not appear to be all that active within the cyber domain whereas some new generation companies operating as support service companies in the outsourced global military and nation-state supply chain do. A key differential here is that such companies would possibly not actually recognise themselves as providing a mercenary type service. However, potentially what begins as a service relationship to a government, or non-state entity operating at a geo-political level, evolves over time through mission creep to become just that. The key defining question for any operation here is ‘what is the strategic intention of the activity/mission?’

An additional consideration is the role of companies which have neither a cyber nor military capability but rather provide services in the information domain. The weaponization of the internet to drive ideological and political narratives and conduct infowars is well documented. However, in the context of cyber mercenary activity we contend that the potency of such operations is less studied and understood than other types of cyber operations. A stand out scholarship in this context is Peter Singer and Emmerson Brooking’s “Like War - The Weaponization of Social Media’ (2018). Similar research includes Thomas Nissen’s work ‘#The Weaponization of Social Media: @Characteristics\_of\_Contemporary\_Conflict’ (2015) and van Niekerk and Maharaj’s article ‘Social Media and Information Conflict’ (2013).

From an African perspective, a case in point would be the role of the ‘influence” (reputation laundering) firm Bell Pottinger. Initially a Public Relations agency, Bell Pottinger gradually became a political influence firm and played a key role in determining the outcomes of both elections as well as military campaigns across the world. Bell Pottinger’s demise came after a highly politicised web driven propaganda campaign in South Africa aimed at challenging a wide ranging narrative of corruption and ‘state capture’ embroiling the then President and his business associates the Guptas. On assignment to the Gupta owned company Oakbay, this was done through a sophisticated influence operation utilising incendiary narratives, bots and sock puppets as well as targeting investigative journalists. The company’s activities took South Africa took the brink of a race war and after being outed by an intensive investigative journalism campaign, ended in the disgrace and bankruptcy of the firm. It is highly doubtful whether any traditional mercenary operation could have had quite as devastating an effect or been able to operate so freely on a comparatively modest budget (Caesar, 2018; Segal, 2018; https://www.influence.film/).

These examples illustrate that we need to re-conceptualise our understanding of what constitutes mercenary activity within the cyber domain. A potentially challenging hurdle is that most cyber and information operations take place well below the threshold of war. This creates a grey area for companies to carry out questionable briefs whilst escaping censure. The Sky News podcast series ‘Into the Grey Zone’ explores some of these tactics.

In terms of outsourcing, cyber advisory companies abound. There are many consultancies which provide bespoke and discreet cyber and intelligence services to states. That per se is not an issue, however it becomes difficult in distinguishing when those services become weaponized. Monitoring the movement and activities of physical mercenary activities is infinitely more straightforward than those in the virtual realm. The delivery of cyber services from dislocated geographies by opaque individuals is an additional complicating factor.

The following quote illustrates the non-traditional nature of a cyber mercenary, as well as the roles such actors can play on behalf of states:

“The NSO Group is now arguing before a US appeal court that it ought to have complete immunity from US anti-hacking laws because it works on behalf of unnamed sovereign government clients. In their rare joint amicus brief filed to an appeal court on Monday night, Google, Microsoft, and others argued against NSO’s appeal, and claimed that offering such legal immunity to the spyware company – or any similar company – posed grave risks to global cybersecurity. The companies said that the consequences of an “immunised and expanded” spyware industry would mean that more foreign governments would have access to “powerful and dangerous” cybersurveillance tools” (Kirchgaessner, 2020).

The supply chain for offensive and intrusive cyber security tools is complex. As the quote above demonstrates, it is also long and usually involves a couple of detours through middlemen and as such it becomes increasingly harder to determine who the culpable part is when tools are misused. Is this the fault of the developers for creating something capable of being weaponized in the first place? Critics would argue that if so, then that applies to every armaments manufacturer worldwide. Others will contend that the responsibility for ethical use lies with the purchaser. The truth is that there is probably responsibility on all parties in this supply chain. Firstly in terms of Know Your Client (KYC) protocols and in regime terms - the human rights records and transparency of governments must surely be a consideration. In truth many producers of known espionage, hacking and exploit tools sell onto distributors without insight into who the intended end user is. Companies which produce such tools and systems are profit making entities and for the most part do not appear to have political goals.

Cyber criminal networks also tend to be profit driven and will sell their offensive code or tools to opaque buyers. Often these networks are so loosely chained that the members of the network do not know one another save for a pseudonym. Different individuals will be deployed at different times depending on the required skill sets. This makes it exceedingly difficult both to take down the entire network as well as attribute blame to the actors. These actors produce both malicious code as well as conduct proxy based espionage and ransomware operations for client groups. These could range from governments to criminals or terrorist groups. A challenge in the proliferation of cyber weapons is that once it has been used, the code can be reversed engineered and used for other purposes. As cyber criminals often sell vulnerability information and exploits themselves, in addition to other components of malware, on the Dark Web, an actor can buy the necessary components or ‘kits’ to build a cyber weapon from different ‘suppliers’. Therefore, no one ‘supplier’ will have visibility of what the code is to be used for.

There are also unpaid actors in cyber space, often motivated by ideological or nationalist reasons rather than money. Cyber troops are most commonly used to fight auxiliary battles in the ‘grey zone’ and conduct information operations. These are non-state actors but frequently act in conjunction with states as force multipliers or cyber militias.

Legitimate tools for security testing can be stolen, and then used or malicious purposes. For example, the security firm FireEye disclosed that it had been hacked and its penetration testing tools had been stolen (Johnson, 2020). Likewise, the WannaCry and NotPetya malware used vulnerabilities stolen from the US National Security Agency (Greenberg, 2017).

1. **What are the motivational factors and strategic intentions of a) clients to recruit “cyber mercenaries” and the type of relationships they may have with them; and b) “cyber mercenaries” and other actors operating alone or through PMSCs in cyber space?**

*Motivational factors can include for instance private gain, material compensation, ideological and other reasons.*

The motivational factors for the recruitment of cyber mercenaries will vary depending on the nature of the actor requesting the service and the nature of the problem which they are trying to address.

In Africa, within the state-sponsored realm, two main drivers would be firstly, to fill a cyber capability gap due to a perceived threat or secondly, to buy in cyber expertise to conduct an identified operation with the added bonus of leveraging the proxy/attribution problem and therefore potentially escaping accountability. We contend that the second scenario is currently rare or undocumented to date as there is minimal incidence of state-sponsored offensive interstate cyber operations by African states. The first scenario on the other hand is a far more likely due to a paucity of cyber skills and warfare capability in many states amidst a diverse and omnipresent threat landscape. The building of state level defensive (or offensive) cyber warfare capabilities is dependent on a robust STEM sector, a solid national ICT industry and significant resourcing of both infrastructure, personnel as well as advanced internet governance and regulation. The lead-time to establish these foundations can be measured in decades rather than years. Suffice to say that the option to pay a third party for a cyber warfare capability and leapfrog directly towards some level of cyber force enablement would therefore be an option that certain states might well consider. This is particularly the case where the cyber threat environment is deemed to be a severe threat to the state.

A third driver may be purely plausible deniability for the state-actor; Brantly (2018) and Borghard and Loneran (2016) indicate this is a prevalent use for state actors. This is to take advantage of the difficulty in attribution in cyberspace, and further complicate attribution through the use on cyber mercenary services. This motivation is also discussed by Collier (2015).

A fourth driver would be to engage either companies or individual hackers for hire for espionage purposes, either domestic or international.

A fifth driver would be to utilise private companies for information operations, as the example of Bell Pottinger described above. This could be to delegitimize opposing political viewpoints or against other states where there are contestations over territory or resources. Peter Pomerantsev illustrates how politicians and states can use communication companies, or organisations specially designed for the purpose, for influence and political ‘smear’ campaigns (2019).

Nation states may also use cyber mercenaries to conduct surveillance on its own citizens. Spyware such as in the NSO example above may be used in order to provide governments with plausible deniability in running unsanctioned surveillance operations that may be against its own laws.

Non-state actors may have similar motivations for hiring cyber mercenary skills: to increase their advantage against competitors and protect themselves against similar measures by their competitors. The use of ‘clandestine’ individuals on the dark web may allow them some plausible deniability if activities such as industrial espionage. Corporations often hire the services of former intelligence and/or military personnel to aid in corporate security and functions for intelligence and counter-intelligence. These operations can conceivable include the hiring of individuals or groups with cyber skills to aid in these functions to provide a competitive advantage. Andrew Brown’s book, ‘The Grey Line: Modern Corporate Espionage and Counter Intelligence’ (2011) discusses this topic in depth. In some instances, states may support their corporations in achieving competitive advantage over international rivals by providing intelligence; or the corporations may gain additional benefit by hacking international competitors (industrial espionage), but also exfiltrate other information to sell to state actors or to gain political favours.

Traditional organised crime hire the services of cyber criminal groups to assist in their operations. For example, a smuggling group used hackers to penetrate the systems of Antwerp port to ascertain where their containers were and to evade custom checks (Bateman, 2013). Organised Crime Syndicates - espionage, infiltration and corruption of bureaucratic networks, data exfiltration to assist in future crimes, theft.

Terrorist and insurgent groups can use cyber skills for influence operations, recruitment, conduct ideological information operations or disrupt and degrade the target’s ability to govern or defend. In addition, they may use cyber crime techniques to fund their real-world operations. These groups may not have sufficient skills in-house, and can contract to individuals or groups to conduct the operations on their behalf. There is also the possibility of states leveraging off insurgent groups with cyber skills to conduct a proxy hybrid war against another nation. Cyber vigilantes could also use such skills for ideological reasons, to embarrass or disrupt the targeted entity and gain public support for a cause. The Anonymous group is well known for ideological attacks against perceived corrupt governments; therefore, they are an ideal group to be used as cyber mercenaries as they will work primarily for ideological reasons.

Where states can use influence and cyber operations against rival state’s political figures, internal political parties can use ‘Cyber Troops’ to degrade and undermine a political adversary. Often these cyber troops can frequently act as proxies for other states. The Stanford Internet Observatory’s ‘More Troll Kombat’ (2020) report on information operations which occurred in Africa but conducted by large powers from outside of the continent. Cyber actors from countries like South Africa and CAR were also utilised to create an authentic basis (Pretorius, 2021).

From these examples, states and non-state actors can be motivated to use cyber actors for plausible deniability and temporarily ‘insource’ skills that they may not have. These cyber mercenaries can be used to perform a range of tasks to achieve certain objectives that will benefit the employer. The cyber mercenaries themselves would provide services for some gain (financial, material, or political favours) or for ideological reasons. Ben Buchanan’s book ‘The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics’ (2020) discusses the use of cyber attacks in geopolitics, and can provide additional detail on this topic.

A challenge presented by these motivational factors is it make distinguishing the types of cyber actors. What is the line between a cyber vigilante and a cyber criminal? This question is discussed by Karen Allen (2020). When does a cyber criminal selling services become a cyber mercenary? If at a technical level the operations are very similar, the main point of distinction becomes the motivation and/or objectives. However, these also appear blurred.

1. **What are the types of cyber-services and products available (e.g., spyware/malware, AI), including their intended purpose in both conflict and non-conflict settings?**

There are a broad range of services and ‘products’ available. As described above, the use of cyber-criminal infrastructure as a proxy is relevant. This infrastructure in the form of botnets for hire can be used for different purposes, such as distributing malware for espionage or future attack, or distributed of denial attacks. In a similar context, the use of bots for broad propaganda and online influence operations could be outsourced to criminal groups or formal consulting organisations. Likewise, a national cyber-security capability, or the development thereof, could be outsourced to a formal cyber-security companies or the defence industrial base who are not necessarily private military or security firms, but could provide the necessary cyber-security expertise for offensive operations on behalf of military or intelligence agencies.

For example, Lunghi (2017) reports that a Libyan cyber-criminal changed to focusing on the distribution of cyber-propaganda. This implies that cyber-criminal groups and infrastructure can be linked to online propaganda, indicating a degree of ‘mercenary’ behaviour as they are providing online services to states in some form of information competition.

In certain contexts, are bug bounty programmes by corporations not a form of employing cyber mercenaries, as individuals or groups are being rewarded for ‘hacking’ the organisation’s systems. This can be extended to a corporation employing services for industrial espionage purposes.

Artificial intelligence is becoming more prevalent in malicious activity, particularly in the generation of deep fakes. There are examples of code freely available on the Internet, allowing those with sufficient skills to reuse and/or modify the code. AI has been used in a successful scam using deep fakes, as well as an AI controlled botnet for DDoS attacks (Damiani, 2019; Bocetta, 2020).

In general, services and products can include (but not limited to):

* Distributed Denial of Service Attacks
* Surveillance and espionage tools
* Malware ‘kits’ for exploits and propagation
* Hacking services
* Social engineering
* Information gathering
* Spam/scam distribution
* Social media bots
* The sale of stolen information and/or vulnerabilities
* Generation of deep-fakes
1. **What role do new technologies play in causing harm remotely in the context of cyber operations, and what are the risks involved? How would you define “directly participating in cyber operations”?**

A challenge of using new technologies in conflict is the uncertainty of the impact ‘battle damage’. With traditional kinetic weapons, the effects are well known and this allows measures to be taken to estimate and limit the damage and possible collateral damage. However, in cyberspace the weapons, such as malware, often spread autonomously, and the effects on computer systems are often uncertain. As a result, malware could easily escape the intended target’s operating environment and affect other networks and systems on a global scale. Examples of how widespread and damaging malware-type of cyber weapons can potentially be include the Stuxnet worm of 2010, and the WannaCry and NotPetya ransomware worms of 2017. As indicated above, AI is being used to enhance the effectiveness of traditional cyber attacks; however, it is also being used to improve threat detection techniques. The Internet of Things (IoT) is introducing vulnerabilities which hackers can exploit. For example, the Mirai botnet was made up of primarily compromised CCTV devices, and in one attack is overloaded Liberia’s national Internet breakout points. In this specific instance, it was a hacker who was hired to target a telecommunications company in the country (Casciani, 2019).

Participating directly in cyber operations would denote intention on the part of the actor. Strictly speaking they would have a sense that they are or are potentially involved in a set of actions which have nefarious purpose in cyber space. This raises the difficult question of whether actors who have unwittingly been involved in such operations could have or should have made a more concerted effort to understand the end purpose of the action or project they were involved in as well as the nature of the parties who contracted them. In the physical realm PMSCs and arms manufacturers are expected to conduct due diligence, be transparent and conduct KYC assessments. Companies in the ITC, consulting and online media and influence sectors are not currently subject to similar charters. Yet it is in these sectors where we see cyber mercenary activities taking place, the key difference being that these industries do not self-identify their activities as being such.

**Regulatory frameworks and their application**

1. **Please provide information on existing national, regional or international legislative, policy and regulatory frameworks, or other initiatives, regarding conduct in cyber space and their application (e.g., transparency, responsible behavior, prevention of prohibited conduct).**

The UN Group of Governmental Experts (GGE) report of 2015 proposed a series of norms related to the responsible use of cyberspace; these are summarised by Esterhuysen, Brown, and Kumar (2019) Several of these norms are directly applicable:

*Norm (a): Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures 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.* (p. 4).

In the context of cyber mercenaries, states should not encourage or make use of cyber mercenaries in a manner that will negatively affect international peace and security, or be harmful to civilian populations.

*Norm (c): States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.* (p. 5)

In the context of cyber mercenaries, states should not harbour cyber mercenaries that are known to have contravened responsible behaviour in cyberspace, nor should they allow infrastructure residing within their sovereign territory to be utilised by cyber mercenaries for such acts.

*Norm (d): States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.* (p. 5)

In the context of cyber mercenaries, states should cooperate to address the threat of cyber mercenaries being used in contravention of responsible behaviour or human rights, and help to prosecute those that do commit such acts.

*Norm (f): A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.* (p. 6)

In the context of cyber mercenaries, states should not make use of cyber mercenary services in such a manner that it could contravene international law or negatively affects critical national infrastructure.

*Norm (e): States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.* (p. 5)

In the context of cyber mercenaries, states should not make use of cyber mercenary services in a manner that could contravene human rights.

Some of the GGE norms may also indirectly apply:

*Norm (g): States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.* (p. 6)

As states need to protect their critical infrastructure, this will include protecting infrastructure from adverse affects resulting from cyber mercenary operations.

*Norm (i): States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.* (p. 6)

States should therefore discourage the use of cyber mercenaries to sell vulnerabilities or offensive tools.

*Norm (j): States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.* (p. 7)

States should therefore discourage the stockpiling of vulnerabilities by cyber mercenary actors.

The Global Commission on the Stability of Cyberspace also proposed norms, in some cases more specific than the GGE norms, and in the other cases, the scope is broader. Those that are relevant include (GCSC, 2019: 21-22):

*1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.*

*2. State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.*

*3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.*

*4. State and non-state actors should not commandeer the general public’s ICT resources for use as botnets or for similar purposes.*

*8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.*

The above five norms limit the targets and activities that can be taken for cyber-operations. This will apply to cyber mercenaries as non-state or state-sponsored actors. However, these norms prohibit what are the ‘ideal’ use-case for cyber mercenaries when employed by a state: to target such infrastructure of national processes and to provide plausible deniability or difficulty in attributing to the state-sponsor. Norm 8 explicitly prohibits non-state actors from conducting offensive cyber-operations; whilst this was primarily in the context of civilian organisations ‘hacking back’, it raises questions as to how cyber-mercenaries will be classified when employed by a nation-state.

*7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.*

The above norm is essentially a broader form of the GGE norm (g) in protecting critical infrastructure and cyberspace.

The Paris Call for Trust and Security in Cyberspace (2018) that signatories should “take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors” (p. 3). The non-state actors working for the purposes of other actors implies a form of cyber-mercenary; however, this clause seems limited to “hacking-back”. There is also a clause on non-proliferation and against harmful actions online; this would indirectly oppose the use of cyber mercenaries to provide offensive tools or conduct operations on behalf of a state or some other actor. Other than these points, *The Paris Call* does not seem to explicitly prohibit the use of cyber mercenaries.

1. **Please provide information on specific national or regional norms and/or regulations governing the provision of security products and services in cyber space by actors operating alone or though PMSCs and other relevant actors.**

Internationally, there is the following conventions that apply to mercenaries and private security:

* African Union (Organisation for African Unity) Convention for the Elimination of Mercenarism in Africa, from 1977.
* United Nations (1989) International Convention against the Recruitment, Use, Financing and Training of Mercenaries.
* Swiss Government (2010) The International Code of Conduct for Private Security Service Providers
* Swiss Government (2008) The Montreux Document

In South Africa, two main pieces of legislation apply to mercenaries and private security:

* Prohibition of Mercenary Activities and Regulation of Certain Activities in Country of Armed Conflict Act 27 of 2006, South Africa
* Private Security Industry Regulation Act 56 of 2001

None of the above conventions and acts explicitly mention their activities in cyberspace, however the clauses could be extended to online activities in addition to real-world activities. It should be noted that some of the documents predate the rise of cyber as an instrument of state power; therefore, they are unlikely to have considered the challenges in the digital age.

In some instances, national legislation is in place to control cyber security technologies or use thereof. For example, the South African Electronic Communications and Transmissions Act (2002) has some regulation for cryptography providers and authentication service providers. Internationally, the Wassenaar Arrangement (1995) seeks to control the export of weapons and dual-use technologies. The updated list (Wassenaar.org, 2020) includes computing, telecommunications and information security technologies.

1. **Please provide information on existing national, regional or international frameworks and mechanisms to investigate, and hold individuals, groups, States or companies accountable for abuses in cyber space, including for espionage, cyber-operations, illegal services or products, and their effectiveness.**

There are a number of frameworks and treaties that apply to the use of technology, define criminal activity online, and/or the repercussions of abuse:

* The Council of Europe (2001) Convention on Cybercrime (The Budapest Convention)
* The African Union (2014) Convention on Cyber Security And Personal Data Protection (Malabo Convention)
* The South African Development Community (SADC, 2011) Model Law on Data Protection

Within South Africa, certain legislature defines cyber crimes and related offences and outlines the repercussions.

* Electronic Communications and Transmissions Act (2002)
* Cybercrimes Bill (2017)
* Protection of Personal Information Act (2013)
* Regulation of the Interception of Communications and Provision of Communication-related Information Act (2002)

**Human rights and IHL impacts of cyber-capabilities and operations conducted by actors operating alone or through PMSCs**

1. **Please describe how the development and use of cyber-capabilities, operations and services (e.g., attacks on digital/physical infrastructure and data, surveillance of individuals) by actors operating alone or through PMSCs can cause and contribute to human rights abuses and violations in non-conflict settings.**
*This includes for instance the rights to life, physical and mental integrity, self-determination, privacy, health, vote, freedom of movement, assembly and association that could be affecting individuals or groups, such as human rights defenders, opposition leaders, or journalists.*

Essentially, the entire digital eco-system is open to misuse and abuse by state and non-state actors. It is important to state that in the presence of sophisticated actors, that the prevention of nefarious cyber operations and services will remain challenging. However, the overwhelming quantum of nefarious activities are not usually sophisticated and are usually enabled by insufficient oversight, regulation and basic security best practices. Countering the range of potential threats calls for robust multi-stakeholder coordination and alignment, particularly private/public partnerships and the full application of the law.

A case in point would be discovery in late 2020 that South Africa’s two largest listed cell phone companies, for a fee, were allowing private investigators and security companies access to their platforms which allowed them to track and trace their subscribers, without their knowledge. Ostensibly, this was to assist in fighting crime however, in terms of legislation, this is in fact illegal. This practice only came to light after the assassination of Lt Col Charl Kinnear, from the Police’s Anti-Gang Unit. Kinnear’s cell phone was pinged 2442 times in the weeks leading to his death in October 2020. As more information emerges it is becoming apparent that these platforms were widely abused and linked to numerous hits and attempted hits and other illegal surveillance activities (Dolley, 2020; Wicks and Cowan, 2020).

The South African National Information Regulator is still awaiting the report from the mobile operators on the activities of WASPS on their networks and the complete failure of corporate governance, ethics, implementation of KYC protocols and subscriber protection. Given the gravity of the abuse more direct action should already have been implemented (MyBroadband.co.za, 2020).

A further question of importance is with regard to the cyber security awareness and competence of security companies as well as their approaches to information security. As these companies deploy additional technologies to improve their security capabilities, they are also expanding the attack surface. This is largely a result of insufficient technical insight and governance oversight. For example, cameras are often installed without testing their software vulnerability to hacking or the changing of the default administrator passwords. As such, web engines like Shodan abound with discoverable camera feeds into homes and offices worldwide (Swart, 2019).

In terms of data privacy, the current legislative framework is insufficient to safeguard the rights of individuals as additional IoT devices are added to the private security eco-system. Sensors and cameras present a specific challenge with regard to the capture and storage of their generated data. For example, private security companies are now sharing footage of their clients property with insurance companies (without notification thereof), ostensibly to combat fraudulent claims (Labuschagne, 2020). The question is who owns the data - the client who contracted the security company and paid for the installation of the cameras and monitoring or the security company?

Examples provided above also illustrate potential abuses of human rights: an individual targeting a telecommunications company effectively blocked an entire nation from the Internet. This could have many ramifications: how many citizens were affected financially due to that act? How many were unable to contact relatives? How many were unable to get medical information or treatment due to the incident? In the example of the NSO spyware, this could be deployed outside of national laws and infringe on individuals’ privacy.

A challenge of cyber attacks is often that vulnerable third-party systems are compromised and used in the attack. This may then degrade the performance of those systems and networks. Where a car can be stolen and used to commit crimes, the owners know that car is stolen as it is physically missing. With cyber attacks, the system is still physically where it should be, however its technical resources are being maliciously utilised to conduct an attack or crime. In that act, how has an organisation or individual been negatively affected?

A problem with the use of ‘proxies’ in to conduct cyber-attacks, is that national leaders (or some other hiring party) may lose the ability to control them (Junio, 2013; Lindsay, 2015). Once a nation has met its objectives, or come to some compromise, the cyber mercenaries may not be satisfied and continue their operations for ideological reasons, or possibly even turn against their former benefactor. This becomes a dangerous situation where the rogue cyber mercenaries may take an ‘at all costs’ approach and infringe on human rights.

1. **Please describe how the development and use of cyber-capabilities, operations and services by actors operating alone or through PMSCs can cause and contribute to breaches of international humanitarian law during armed conflicts and its impact on civilian populations.**

A recurrent and vexatious question in cyber warfare is the question of what constitutes an attack and where the threshold of such an attack is in order to constitute a violation of IHL. Problematically, the vast majority of cyber attacks and cyber warfare operations occur below the threshold of war. Protagonists have become adept at exploiting this in order to avoid possible censure.

“Some operations are easier to define as "attacks" than others. It is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL. In the ICRC's view, this includes foreseeable indirect (or reverberating) effects of death, injury, or physical damage” (Horowitz, 2020).

In terms of IHL, the ICRC advocates the position that cyber attacks which target three specific categories would result in civilian harm and therefore violate the Geneva Convention which prohibits the use of weapons which are indiscriminate by nature. “Notably, any use must respect the principles of distinction, proportionality and precautions. In particular, attacks must not be directed at civilians or civilian objects. Critical civilian infrastructure—including the cyber infrastructure on which they operate or rely—are civilian objects and therefore protected against attack, unless they have become military objectives.” (Gisel and Olejnik, 2018).

Three key areas present cause for concern with regard to cyber attacks. These are:

* Attacks against the healthcare sector
* Attacks on Critical National Infrastructure
* Cyber attacks which present systemic risk - for example national and international financial systems.

 “For Africa’s people, cyber operations, which are inherently destabilizing, pose a threat to some of the world’s most vulnerable populations and fragile States. This places already exposed populations at risk of potentially devastating consequences in the event of a major cyber incident. Key concerns are the consequences of a cyberattack on the growing number of nuclear energy sites or attacks on water storage and hydroelectric entities. Africa is one of the world’s hardest hit regions in terms of climate change, and drought has become an ever-present phenomenon. Any loss of water or contamination will thereof have dire consequences, notably disease and famine. Digital money platforms also present a high value target as these drive the remittances from the African Diaspora to home countries and annually push billions of dollars to some of the world’s most impoverished and underserved communities. In many instances such platforms have replaced cash and formal banking and are critically reliant on zero internet redundancy. For States with weaker cyber security capacities, a strong legal and normative framework is an essential element affording protection from foreign interference and cyber threats. Affirming existing international law, including international humanitarian law, may also shield States against becoming ‘collateral damage’ in cyber operations conducted elsewhere. The impact of a cyberattack on South Africa’s ESKOM energy grid is a case in point – eight countries in the SADC region are reliant on the grid. Experts estimate that in the event of a grid failure, it will take between one and six weeks to restart it; as there is no other power source to bootstrap onto, a black start would be required as South Africa constitutes a ‘power island’. Such an event would be an unimaginable catastrophe for an entire and vast region” (van der Waag-Cowling, 2020)

It is further submitted that the current IHL framework may be too limited in its potential application in the case of cyber operations and their effects. Currently the focus remains on the end result as a kinetic effect for determining violation of IHL. In the digital world however, this bar is arguably too high. The increasing prevalence of information operations which affect political stability and free and fair elections undermine democratic processes as well as the right to self determination. For fragile states and young democracies, this poses a substantial and ever increasing threat.

Detailed discussions on IHL and cyber operations can be found in the Tallinn Manual 2.0 (Schmitt, 2017), François Delerue’s book ‘Cyber Operations and International Law’ (2020), and Russel Buchan’s book ‘Cyber Espionage and International Law’ (2018).

**References**

African Union (Organisation for African Unity). (1977) Convention for the Elimination of Mercenarism in Africa, https://www.peaceau.org/uploads/convention-elimination-mercenariism-en.pdf

African Union (2014) Convention on Cyber Security and Personal Data Protection (Malabo Convention), https://www.opennetafrica.org/?wpfb\_dl=4

Allen, K. (2020) When digital vigilantism turns into cybercrime, Institute for Security Studies, https://issafrica.org/iss-today/when-digital-vigilantism-turns-into-cybercrime

Bateman, T. (2013) Police warning after drug traffickers' cyber-attack, BBC, https://www.bbc.com/news/world-europe-24539417

Bocetta, S. (2020). Has an AI Cyber Attack Happened Yet? https://www.infoq.com/articles/ai-cyber-attacks/

Borghard, Erica D, and Shawn W Lonergan. 2016. “Can States Calculate the Risks of Using CyberProxies?” Orbis 60(3): 395–416.

Brantly, A.F., (2018) The Cyber Deterrence Problem, 2018 10th International Conference on Cyber Conflict, 31-54.

Brown, A. (2011) The Grey Line: Modern Corporate Espionage and Counter Intelligence, Amur Strategic Research Group.

Buchan, R. (2018) Cyber Espionage and International Law, Oxford: Hart Publishing.

Buchanan, B., (2020) The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Cambridge, MA: Harvard University Press.

Caesar, E. (2018) The Reputation-Laundering Firm That Ruined Its Own Reputation, The New Yorker, https://www.newyorker.com/magazine/2018/06/25/the-reputation-laundering-firm-that-ruined-its-own-reputation

Casciani, D. (2019) Briton who knocked Liberia offline with cyber attack jailed, BBC, https://www.bbc.com/news/uk-46840461

Collier, J. (2015) State Proxies & Plausible Deniability: Challenging Conventional Wisdom, Cyber Security Intelligence, https://www.cybersecurityintelligence.com/blog/state-proxies-and-plausible-deniability-challenging-conventional-wisdom-644.html

The Council of Europe (2001) Convention on Cybercrime (The Budapest Convention), ETS No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Cybercrimes Bill 6 of 2017, South Africa, https://static.pmg.org.za/parl-bills-B6D-2017-GJ\_B6D-2017-GJ.PDF

Damiani, J. (2019) A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. Retrieved from Forbes: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=1afde0f32241

Delerue, F. (2020) Cyber Operations and International Law, Cambridge: Cambridge University Press.

Dolley, C. (2020) Hide and seek: into the murky world of cellphone tracking, Daily Maverick, https://www.dailymaverick.co.za/article/2020-11-21-hide-and-seek-into-the-murky-world-of-cellphone-tracking/

Electronic Communications and Transmissions Act 25 of 2002, South Africa, https://www.gov.za/documents/electronic-communications-and-transactions-act

Esterhuysen, A., Brown, D., and Kumar, S. (2019, 19 December). Unpacking the GGE's framework on responsible state behaviour: Cyber Norms, Global Partners Digital and Association for Progressive Communications, https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/

Gisel, L., and Olejnik, L., (2018) The potential human cost of cyber operations: Starting the conversation, Humanitarian Law and Policy, ICRC Blog, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/

Global Commission on the Stability of Cyberspace (2019, November). Advancing Cyberstability, https://cyberstability.org/report/

Greenberg, A. (2017) Hold North Korea Accountable for WannaCry—And the NSA, Too, Wired Magazine, https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/

Horowitz, J., (2020) Cyber Operations under International Humanitarian Law: Perspectives from the ICRC, ASIL Insights 24(11), https://www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc

Johnson, D.B. (2020) FireEye hacked, red team tools stolen, SC Magazine, https://www.scmagazine.com/home/security-news/apts-cyberespionage/fireeye-hacked-red-team-tools-stolen/

Junio, T.J. (2013) How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. Journal of Strategic Studies 36(1), 125–33.

Kirchgaessner, S. (2020) NSO Group spyware 'dangerous', say tech firms in legal filing, The Guardian, https://www.theguardian.com/us-news/2020/dec/22/nso-group-spyware-dangerous-say-tech-firms-in-legal-filing

Labuschagne, H., (2020). Vumacam footage being used in insurance claims investigations, MyBroadband.co.za, https://mybroadband.co.za/news/security/373269-vumacam-footage-being-used-in-insurance-claims-investigations.html

Lindsay, J.R., (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, Journal of Cybersecurity 1(1), 53-67.

Lunghi, D. (2017, 16 October) “From Cybercrime to Cyberpropaganda,” Trend Micro, http://blog.trendmicro.com/trendlabs-security-intelligence/from-cybercrime-to-cyberpropaganda/

Maurer, T. (2018) Cyber Mercenaries: The State, Hackers and Power, Oxford: Oxford University Press.

MyBroadband.co.za, (2020) Vodacom and MTN can face legal action over Kinnear murder, https://mybroadband.co.za/news/cellular/372354-vodacom-and-mtn-can-face-legal-action-over-kinnear-murder.html

Nissen, T.E. (2015) ‘#The Weaponization of Social Media: @Characteristics\_of\_Contemporary\_Conflict, Danish Defence College, https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media

The Paris Call for Trust and Security in Cyberspace (2018). https://pariscall.international/en/

Pomerantsev, P. (2019) This is Not Propaganda: Adventures in the War Against Reality, London: Faber & Faber.

Pretorius, L., (2021) Anatomy of a disinformation campaign: The who, what and why of deliberate falsehoods on Twitter, Daily Maverick, https://www.dailymaverick.co.za/article/2021-02-09-anatomy-of-a-disinformation-campaign-the-who-what-and-why-of-deliberate-falsehoods-on-twitter/

Prohibition of Mercenary Activities and Regulation of Certain Activities in Country of Armed Conflict Act 27 of 2006, South Africa, https://www.gov.za/documents/prohibition-mercenary-activities-and-regulation-certain-activities-country-armed-conflict#

Protection of Personal Information Act 4 of 2013, South Africa, https://www.gov.za/documents/protection-personal-information-act

Private Security Industry Regulation Act 56 of 2001, South Africa, https://www.gov.za/documents/private-security-industry-regulation-act

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, South Africa, https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

Segal, D. (2018) How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa, The New York Times, https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html

Singer, P.W. and Brooking, E. (2018) Like War - The Weaponization of Social Media, New York: Hougton Mifflin Harcourt.

The South African Development Community (2011) Model Law on Data Protection, http://www.itu.int/ITU-D/projects/ITU\_EC\_ACP/hipssa/docs/SA4docs/data%20protection.pdf

The Stanford Internet Observatory and Graphika, (2020) More Troll Kombat, https://public-assets.graphika.com/reports/graphika\_stanford\_report\_more\_troll\_kombat.pdf

Swart, H., (2019) Visual surveillance and weak cyber security, Part One: When cameras get dangerous, Daily Maverick, https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/

Swiss Government (2008) The Montreux Document, https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/montreux-document.html

Swiss Government (2010) The International Code of Conduct for Private Security Service Providers, http://observatoire-securite-privee.org/en/content/international-code-conduct-private-security-service-providers-icoc

United Nations, (1989) The International Convention against the Recruitment, Use, Financing and Training of Mercenaries, General Assembly Resolution 44/34, https://www.ohchr.org/EN/ProfessionalInterest/Pages/Mercenaries.aspx

UN News, (2019) World must do more to tackle ‘shadowy’ mercenary activities undermining stability in Africa, says UN chief, https://news.un.org/en/story/2019/02/1031931

van der Waag-Cowling, N., (2020) Living below the cyber poverty line: strategic challenges for Africa, Humanitarian Law and Policy, ICRC Blog, https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/

van Niekerk, B., and Maharaj, M. (2013), Social Media and Information Conflict, International Journal of Communication, vol. 7, 1162–1184.

Wassenaar Arrangement (2020) List of Dual-Use Goods and Technologies and Munitions List, https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

Wicks, J., and Cowan, K., (2020) Targeting AGU Team C: How Zane Kilian Tracked Anti-gang Cop Charl Kinnear and his Team, News24, https://specialprojects.news24.com/zane-kilian-charl-kinnear-cellphone-tracking/index.html

Further Reading

Buchanan, B. (2017) The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Oxford, Oxford University Press.

Harris, S. (2015) @War: The Rise of the Military-Internet Complex, Boston: Eamon Dolan/Mariner Books.

Kaplan, F. (2017) Dark Territory: The Secret History of Cyber War, New York: Simon & Schuster.

Ramluckan, T., Wanless, A., and van Niekerk, B. (2019) Cyber-Influence Operations: A Legal Perspective, 18th European Conference on Cyber Warfare and Security, 379-386.

Segal, A. (2016), The Hacked World Order, New York: Hachette.

van der Waag-Cowling, N. (2018) South Africa and the Cyber Warfare Threat: A Strategic Overview, in: Wells, B. (ed.), Civil-Military Cooperation and International Collaboration in Cyber Operations, Dahlonega:UNG Press, pp 22-51.

van der Waag-Cowling, N. (2019) Africa must harness the potential of Cyber Power and Digital Diplomacy, http://www.sun.ac.za/english/faculty/milscience/sigla/Documents/Briefs/Briefs%202019/Brief%2011.pdf

van Niekerk, B., and Maharaj, M. (2013) Information-Based Conflict in Africa, Scientia Militaria South African Journal of Military Studies, 41(2), 24-41.

van Niekerk, B., (2018) Information Warfare as a Continuation of Politics An analysis of cyber incidents, 2018 Conference on Information Communications Technology and Society (ICTAS), https://ieeexplore.ieee.org/document/8368758