Inputs: Report on The Provision of Military and Security Cyber Products and Services by 'Cyber Mercenaries' and Its Human Rights Impact

Submitted by Usalama Reforms Forum

Usalama Reforms Forum is a Kenyan based Public Safety Research and Innovation Organization founded as a Police Reforms lobby in 2008 with the mandate of consolidating civil society engagement in the security sector reforms programs in the country.

P.O. Box 27461, 00100

Nairobi, Kenya

Cell:+254 721 967 932/+254725150643

email:caleb.wanga@usalamaforum.org

info@usalamaforum.org

website: www.usalamaforum.org

I. Definition and overall risk of cyber mercenary behavior

In recent years, the risk of human rights violations is increasing with the development of new technology and in the means of cyber attacks. State actors may employ private entities, whether private military/security companies or cyber technology companies, to collect data of government institutions, and even citizens, which in fact violates the relevant human rights protection principles of the United Nations. However, the concept and regulation of cyber mercenaries need to be further discussed and refined. The stakeholders of cyber mercenaries involve not only state actors, but also private institutions and individual actors, such as cyber hackers or organized institutions, who are employed by some governments to carry out cyber attacks in order to achieve the purpose of the state actors or business enterprises to spy on potential competitors. The traditional concept of sovereignty is further extended to "cyberspace sovereignty".

Up to now, there is no consensus on the concept of cyber mercenary. Referring to the traditional definition of mercenary, cyber mercenary needs two main conditions: one is that the emissary or ultimate beneficiary behind cyber mercenary is a government or state actor. Second, the state actors entrust private organizations such as cyber technology companies and individual actors (hackers) to carry out cyber attack or operations, so as to achieve the purpose of the state actors' instigation.

Relevant UN resolutions and current international regulation prohibit state actors from using mercenaries to carry out offensive or hostile actions in order to avoid violations of human rights of host countries and local communities. Countries have generally reached a consensus on the harm of traditional mercenaries to human rights violations, and

recognized relevant resolutions and international rules. The regulations on the use of private security companies in international complex environment and vulnerable areas have also formed such rules as "Montreux document" and "international code of conduct for private security service providers". Their common goal is to clarify the responsibilities and international compliance obligations of mother country, host country and private security service providers, so as to promote the protection of human rights.

II. Main cases of cyber mercenary behavior and related countries' legislation

The clients and beneficiaries of cyber mercenaries can include state and non-state actors who have signed up with "cyber mercenaries", as well as other actors operating alone or through private military and security companies to acquire cyber capabilities. Through defense contracting, military security departments, private enterprises and even individual actors form a very large cyber security industry complex. Both state and non-state actors may benefit from cyber capabilities and actions. In particular, the countries concerned are integrating cyber capabilities into most of their operational areas, including military and anti-criminal activities. Relevant countries use cyber capabilities to monitor leaders, critics, journalists and other human rights defenders in other countries. It is said that some countries have also used agents to attack government computer systems in order to collect sensitive security and defense information and to sabotage key infrastructure. In addition, the state and / or its agents have been accused of disseminating erroneous/rumors information affecting elections and the democratic process.

1. Cyber security and attack

In view of the obvious advantages and even monopoly position of big powers in the fields of cyber technology, they are more advanced and frequent in smaller or less advanced countries to conduct cyber defense and attack.

Although it is difficult to judge the extent to which these cyber defense contractors have participated in the relevant national cyber military operations from the public information, there is no doubt that the above "products and services" have touched on the "essentially exclusive state functions", which are closely related to public interests and should have been prudently performed by the government staff on behalf of the authority of the governments. [1]

The revolving door mechanism

The revolving door mechanism between public and private sectors provides institutional guarantee for the development of cyber security industry complex. There is a frequent flow of personnel among the army, security agencies and cyber defense contractors.

Recently, personnel changes from non-military departments to cyber defense contractors are more frequent. This "revolving door" mechanism skillfully combines the cyber security needs of the public sector with the advantages of human resources of the private sector, and reduces the transaction cost caused by information asymmetry.

The public-private collaboration

The essence of cyber security industry complex is public-private cooperation and civil military integration. It reduces costs, improves efficiency, and helps the country to establish and maintain the power of cyberspace control. To a certain extent, leaving the relevant cyber

[1] http://www.thespywhobilledme.com/the_spy_who_billed_me/2007/12/cia-contractors.html

security business to private enterprises can bypass the red tape inherent in the state bureaucracy, and help to deal with those things that the state security departments need to deal with but should not come forward in person. [2]

The vulnerability of medium-sized businesses

The COVID-19 has further promoted the intensification of cyber attacks. According to the state of SMB cybersecurity at a time of crisis by PwC, only 27% of small and medium-sized businesses (SMBs) have a dedicated cybersecurity team, while 57% of them had experienced an online attack in the last 24 months. Viruses and malware (51%), web-based attacks (38%) and phishing attacks (32%) were identified as the top-three cyberattacks on SMBs. Most SMBs respondents express confidence in their cybersecurity measures, but only 53% of them have antivirus solutions in place - indicating that many have not deployed the most basic cybersecurity tools. 76% of SMBs sustained more than one cyberattacks over the last 24 months. [3]

2. Dissemination of fake news and information

Private information technology companies are deeply involved in the cyber defense of national government departments. The products or services they provide include: cyber information monitoring, including the development of monitoring software, and data mining of intercepted text and audio-visual information. Cyber weapon development: by checking the current computer system vulnerabilities, the development of weapons for cyber attack and defense. Participate in cyber military operations, including undertaking cyber defense, providing cyber

[3] https://www.pwccn.com/en/press-room/press-releases/pr-150720.html

military training, support and strategic and tactical consultation. Through the private sector, entrusted by the government departments, they participate in using the Internet information and UAV to physically attack political leaders of some countries (including those happened the Middle East countries), spread in the Internet fake news and information to impact public opinion and democratic election.

The Iraq war case

During the Iraq war, the U.S. Department of Defense hired Lincoln group, a private defense contractor, to send news prepared by the U.S. military to 12 to 15 Iraqi and Arab newspapers and media for publication, and paid monthly for the replicators. Lincoln group claims that it has put more than 1000 articles in Iraqi and Arab newspapers, published editorials on Iraqi websites, and used private contractors to help blur the boundaries between government and private, insulate government monitoring, and achieve the purpose of overturning Iraq's policies through false intelligence and propaganda. [4]

The Zimbabwe fake news mercenaries

According to the press in July, 2018, HARARE, Zimbabwe, Zimbabwe opposition leader and presidential candidate Nelson Chamisa has accused the ruling party of hiring people to spread false stories about him in order to influence crucial and historic vote. Chamisa said the government has "hired what are called fake news mercenaries" as the July 30 election drew near. [5]

The Indonesian election case

An investigation by Reuters showed both major political camps in 2019

[4] Gerald Sussman, Branding Democracy: U.S. Regime Change in Post-Soviet Eastern Europe. New York: Peter Lang, 2010

[5] Zimbabwe's Opposition Leader Accused The Ruling Party Of Hiring "Fake News Mercenaries". https://www.buzzfeednews.com/article/tamerragriffin/zimbabwe-fake-news

were paying shadow operatives to produce slanted content, often attacking opponents with misleading or fabricated information. There have been many examples of false information going viral during this campaign and being fanned by supporters of both President Joko "Jokowi" Widodo and rival candidate Prabowo Subianto. Claims and rumours have damaged them both, including erroneous suggestions that Jokowi is a Christian or a communist, or that Prabowo would abolish the military or promote polygamy. Facebook has enormous influence in Indonesia with more than 130 million users; it is one of the social media giant's largest markets in the world. And its platforms, including WhatsApp and Instagram, have been fertile ground for the spread of misinformation. As a result, Indonesia has become a key focus for the company. On Apr 12, 2019, it announced it had removed 234 accounts "for engaging in coordinated inauthentic behavior". "This is an addition to a similar announcement in January, when we disrupted a network of accounts that were linked to the Saracen Group, and removed them from the platform," a Facebook spokesperson told.[6]

3. Data security and leakage

In the era of big data, data leakage events emerge one after another, and data security has become one of the main factors hindering the development of big data. In the past 10 years, many global technology giants, especially financial institutions, have suffered serious data security and information leakage events.

The LinkedIn leakage case

On April 7, 2021, LinkedIn, with more than 700 million registered users,

[6]https://www.channelnewsasia.com/news/asia/indonesia-election-fake-news-war-room-fighting-political-hoaxes-11439398

suffered a large-scale data leakage. The data packets of 500 million LinkedIn users were sold on hacker forums. The leaked data included the user's name, e-mail address, telephone number, workplace information, etc.

The Muslim Pro and X-Mode case

It is reported that military is buying the granular movement data of people around the world, harvested from innocuous-seeming apps, Motherboard has learned. The most popular app among a group Motherboard analyzed connected to this sort of data sale is a Muslim prayer and Quran app that has more than 98 million downloads worldwide. Through public records, interviews with developers, and technical analysis, Motherboard uncovered two separate, parallel data streams that military uses, or has used, to obtain location data of potential threats.

Regulation progress on cyber attack

In recent years, in order to provide legal protection for personal privacy, countries have stepped up the legislative process in the field of cyberspace and data. In 2018, the EU issued the general data protection regulation (GDPR), which clearly stipulates that the data controller shall perform the obligation of informing the data owners. GDPR gives the data owners a wide range of control over its data, including the right to know, access, correct, delete, limit processing, portability, objection and so on. For example, in data collection, the data controller should provide the data owners with the identity and contact information of the data controller, the purpose and legal basis of data processing, and the rights of the data owners in a concise, transparent, accessible way. In 2013, NATO cyber defense cooperation center of excellence launched "Tallinn Manual version 1.0", which

mainly explains and discusses the application of armed conflict law to cyberspace. Tallinn Manual is the world's first rule of international cyberspace law formulated by NATO's Center of excellence in Cooperative Cyber Defense (CCD COE), which makes cyber security an important part of safeguarding national sovereignty. Based on international regulation and the technical characteristics of the Internet, this manual puts forward a general legal framework for the exercise of the right of self-defense in cyber attacks. At the same time, it also discusses and explains the controversial issues. Its adaptability mainly aims at the wartime environment and the conflict of cyber attacks between states.

4. Privacy and cyberstalking

The current concept of data governance is relatively broad, and there is no internationally accepted data governance rules in peacetime. When we focus on the issue of cyber mercenaries, we need to define whether it constitutes an act of war? Many cyber attacks take place in peacetime, not during military armed conflict. Therefore, whether the scope of "cyber mercenary" behavior will extend to the broader content of data governance in peacetime, or even further broaden the concept of "cyber mercenary".

The prism gate incident

As a former employee and technology contractor, Snowden disclosed to the Guardian and the Washington Post in June 2013 the secret documents of the prism secret surveillance project launched by the US National Security Agency and the FBI in 2007, and directly went to the central servers of US internet companies to mine data and collect intelligence, including Microsoft, Yahoo, Google, Microsoft, etc, Nine international

network giants are involved in the analysis of personal contact information and actions from audio, video, pictures, e-mail, documents and connection information. On November 18, 2013, Harris, a world-famous investigation organization, released data in a public opinion poll. In the six months since the prism gate incident, in order to protect personal privacy, 80% of Americans have changed their social network account settings. On May 30, 2021, the Danish National Broadcasting Corporation (DR) broke out a major scandal. From 2012 to 2014, the National Security Agency (NSA) used the eavesdropping system of Danish intelligence agencies to monitor senior officials in Sweden, Norway, France and Germany, including German Chancellor Angela Merkel and German President Steinmeier. [7]

The Swiss-based cryptological equipment manufacturer

In March, 2020, Switzerland's Federal Department of Finance has filed a criminal complaint "against persons unknown" over media reports that a leading Swiss-based cryptological equipment manufacturer was secretly owned by the United States Central Intelligence Agency (CIA). The complaint relates to Crypto AG, the world's leading manufacturer of cryptologic equipment during the Cold War, whose clients included over 120 governments around the world. The secret deal, dubbed Operation RUBICON, allegedly allowed the US and West Germany to spy on the classified government communications of several of their adversaries —and even allies, including Austria, Italy, Spain, Greece, Jordan, Saudi Arabia and the United Arab Emirates. [8]

The NSO group case

At present, Israel is one of the countries with the most developed private cyber technology. Among the world's leading intelligent cyber

[7] https://www.euronews.com/2021/05/31/did-denmark-help-the-u-s-spy-on-european-leaders
[8] https://intelnews.org/2020/03/03/01-2730/

companies, there are more than 300 companies in Israel, covering all aspects of service from bank financial security to key infrastructure. NSO group is a leader in the field of cyber warfare. Cooperating with the military and homeland security departments, it can enhance the technical capabilities of partners in the field of cyber warfare, whether in defense or attack. In 2014, Francisco partners Management LLC, a private equity firm in San Francisco, acquired NSO at a price of 145 million Australian dollars (about 111 million US dollars). In 2015, a local Panamanian media reported that the Panamanian government bought the Pegasus spy program and paid a $10.6 million to NSO for "information collection for mobile devices". At that time, the New York Times published an article saying that the Panamanian government's move was to monitor Rafael Cabrera, a Mexican journalist who had previously focused on exposing the government's conflict of interest. In 2019, the NSO group was sued by Facebook for violating the computer fraud and abuse act. According to the litigation documents submitted by both sides to the federal court, from April to May 2019, the NSO group deployed Pegasus software to about 1400 mobile devices equipped with WhatsApp software. Facebook claims that nearly 100 human rights advocates, journalists and members of civil society around the world have been targeted. On December 23, 2020, Microsoft officially declared war on NSO group. Tom Burt, vice president of Microsoft's customer security and trust department, said publicly on the Internet that the NSO group is the largest cyber mercenary in the 21st century, and they should not be granted any immunity.

III. The impact of Cyber mercenaries on human rights and international humanitarian law

Cyber mercenary behavior involves new means of violating human rights, which all involve international level monitoring and regulation. From the perspective of third-party monitoring, there is no doubt that the government needs to participate in or even lead the monitoring process, but it still needs the participation of professional technology companies and other third-party institutions. As for the regulatory focus, no matter at the domestic level or the international level, it involves how the government, enterprises and third parties strengthen cooperation, and ultimately it should be put down to legislation and regulatory implementation. From the perspective of stakeholders, we need to consider all aspects of the industry chain, and finally form a convention or international regulation mechanism. Based on the analysis of stakeholders, monitoring differs from country to country, so it is very difficult for the international collaboration on cyber mercenary monitoring.

The current definition of mercenaries

According to the International Convention Against the Recruitment, Use, Financing and Training of Mercenaries (UN A/44/34), the definition of A mercenary in Article 1 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 ranks 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. The

Article 2 makes it clear that any person who recruits, uses, finances or trains mercenaries, as defined in article 1 of the present Convention, commits an offence for the purposes of the Convention.[9]

Possible definition of cyber mercenaries

Scope of cyber mercenary behavior is easy to be generalized and vague. At present, most of the traditional private military security companies do not master the professional cyber attack and defense technology, and may take action through the merger and acquisition of some cyber security technology companies. The concept of cyber mercenary may be generalized, and monitoring blurred.

Recognizing the common sense of difference between legal status of "private security companies"(PSCs) and "mercenaries", the main lies in the purpose of defense or attack. The Montreux document and ICoC (international code of conduct for private security service providers) are mainly regulating PSCs for providing defensive security services in compliance with human rights and humanitarian law, rather than aggressive behaviors. However, the mercenaries are usually employed for offensive purposes, which make it illegal under the current international regulation status.

When the private military security companies enter the cyber field and provide new security services in cyberspace, their business scope has changed from a defense oriented business to an offensive oriented behavior. The cyber mercenary behavior is in an offensive dominated cyberspace environment.

Suggestions for regulation and monitoring

In view of the above analysis, from the perspective of regulatory

[9] the International Convention Against the Recruitment, Use, Financing and Training of Mercenaries https://documents-dds-ny.un.org/doc/UNDOC/GEN/N89/299/34/IMG/N8929934.pdf?OpenElement

framework, there are many stakeholders, involving governments, private institutions, individuals (hackers), product providers in the grey / dark network, etc. There are a wide range of activities related to cyber security act and attacks, such as attacks on digital and physical infrastructure and data, and personal surveillance, which may affect human rights such as the right to life, the right to physical and mental integrity, the right to self-determination, the right to privacy, and the right to health. To this end, the following suggestions are put forward for the reference of the working group:

1) Define cyber mercenary based on the current definition of a traditional mercenary. The possible definition should include the following key contents: first, the participation of state actors; Second, there is recruitment relationship; Third, the implementation of hostile offensive behavior. When defining a cyber mercenary, we can retain the basic connotation of traditional mercenary and add the content characteristics of its use of new technology and cyber attack as a means.

2) Strengthen the monitoring of cyber mercenary behavior particular in illegal data/software trading and cross-border transactions. Learning from the relevant international legislative model and content of the arms trade treaty, we urge the exporting and importing countries to cooperate to prevent the illegal transfer of data and software, so as to become a new attack weapon used by cyber mercenaries.

3) Strengthen regulation and legislation in prevention and protection of cyber attack on key infrastructure and personal data privacy. Cyber attack can easily make a country's power system, financial system, oil and gas pipeline control system paralyzed, and serious

impact to national security, social stability and wellbeing of people, it is important to form an international legal consensus on preventing cyber attack on key infrastructures and strengthen the supervision and crackdown on personal information leakage and data trafficking, so as to promote national security, and privacy protection.

4) Further research and consult to clarify the whole industrial chain of cyber mercenaries. In reality, there may be multi-layer subcontracting and entrustment between state actors and private entities, which makes the stakeholders behind the scenes very hidden. In terms of regulatory capacity, even if an international convention is to be formed in the future, implementation will be subject to the cooperation of a variety of actors and experts. It seems necessary to build an international regulatory mechanism of multi stakeholder co-governance.

5) Actively call on participation in the construction of the global governance system of cyber mercenaries. In view of the current chaos in the governance of cyber mercenaries, we should adhere to multilateralism and oppose unilateralism and power politics in the field of international regulation and legislation of cyber mercenaries, firmly safeguard the international system with the United Nations as the core, promote dialogue and consultation among governments, and invite multiple stakeholders to participate in the negotiation and formulation of relevant rules. To urge the international community to establish a judicial collaboration system and an international joint law enforcement mechanism to prevent and combat cyber mercenary acts, intensify the condemnation and crackdown against cyber mercenary acts and their related stakeholders behind the scenes, and carry out mutual cooperation

and joint crackdown on Transnational cyber mercenary acts.

6) Further refine concept of "cyber mercenary" and related behavior on its impact on violation of human rights and humanitarian laws. The relevant concepts should be more accurate and clarified, so as to avoid politicization and ideologization of the issue of cyber mercenary, and even becoming a way to unilaterally abuse and implement international sanctions resolutions. It is important to actively promote the protection of human rights in accordance with the current international regulation and under the multilateral negotiation framework of the United Nations.

Reference links:

1. https://en.wikipedia.org/wiki/Central_Intelligence_Agency
2. http://www.thespywhobilledme.com/the_spy_who_billed_me/2007/12/cia-contractors.html
3. https://webcache.googleusercontent.com/search?q=cache:53LvGiPj8pEJ:https://www.washingtonpost.com/investigations/top-secret-america/2010/07/18/methodology-credits/+&cd=1&hl=zh-CN&ct=clnk
4. https://www.washingtonpost.com/investigations/top-secret-america/2010/07/18/methodology-credits/
5. https://www.uscnpm.com/model_item.html?action=view&table=article&id=5003
6. https://www.euronews.com/2021/05/31/did-denmark-help-the-u-s-spy-on-european-leaders