Guidelines For Prevention

Of

Online Abuse And Harassment

In

Ghana

Date: 18th October, 2020

Contents

1. Introduction 4
2. Evolution of Online Abuse and Harassment in Ghana 5
3. Factors sustaining online abuse and harassment in Ghana 5
4. Sanitization of the Cyber Space 6
5. Target audience of the guidelines 7
6. Methods used to course Online abuse 8
7. Punishment for online offenders 9
8. Measures to enhance cyber hygiene 10
9. Forms of rehabilitation Support for the Abused 11
10. Definitions 11
1. Appendix 12

Acronyms and Abbreviations

CSOs	-	Civil Society Organisations
CHRAJ	-	Commission for Human Rights and Administrative Justice
GDP	-	Gross Domestic Product
ICT4D	-	Information and Communications Technology for Development
ID	-	Identification
IT	-	Information Technology
MTN	-	Mobile Telephone Network
NDBCA	-	National Data Base of Cyber Abusers
PC	-	Personal Computer
RAa	-	Research Agencies
R&D	-	Research and Development
USD	-	United States Dollars

1. Introduction

1.1 The purpose of the guidelines is to provide a guide for the prevention of online abuses and harassment in Ghana in line with the Electronic Transactions Act, 2008 (Act 772), the Electronic Communications Act, 2008 (Act 775) and the Data Protection Act, 2012 (Act 843), hereinafter referred to as "the Acts." The guidelines shall apply to online activities of individuals and Organizations operating in the cyberspace of Ghana. In specific, the guidelines seek to ensure that individual or group using online services in the country do so in a safer environment and not suffer unnecessary abuse and harassment of others.

1.2 The internet evolution is fast changing the topography of national security and its management thereof. Many hold the view that the internet epoch dubbed the ICT4D is stifling the sovereign power countries to curtail interference in their domestic affairs by other nationals. This is a result of the cyberspace being transnational, and no individual country is able to unilaterally curb its menace. The transnational nature and other factors- weak cyber legislation, funding gaps, inadequate skills, equipment, significant procedural hurdles and training- is impacting deleteriously on individual State's ability to perform its sacred duty of protecting its sovereign interest within the cyberspace.

1.3 Others, however, are of the view that the internet revolution is helping to strengthen national and global democratic governance. It has also enabled the sharing of information, exchange of ideas, facilitate trade, and business, and help reduce poverty and assist improve healthcare services. In many countries, including Ghana, the internet is creating an opportunity for greater participation in the global economy.

1.4 However, there are severe challenges that come with the influx of technology and need stressing, and many governments are finding it hard to grapple with. The cyber threat to national security is viewed from three angles: - internet used by dangerous organizations for disruptive purposes, to attack targeted country's critical infrastructure and the threat of networked information system disablement and possible debilities. These issues are complex, transnational and require a high level of technological savviness and sophistication to find solutions to them. Cyber developments are also creating enormous global cost and seem unlikely to slow owing to lax technology use and significant benefits from engaging in cybercrimes. As of 2016, the global cost of cybercrimes stood at USD600.0 billion (0.8% of global GDP). This represents a steady growth from a 2014 estimated cost of $345- $445 billion (0.6% of GDP).

1.5 Ghana's desire to sanitize its online space has been to ensure that citizens are free from any form or shape of abuse and harassment from domestic and external sources. To this end, over the years' conscious efforts have been made through the creation of awareness and building capacity of citizens to manage better their cyber activities and how to manage related challenges with their use of internet infrastructure.

1.6 However, abuse and harassment of users of cyber services have received less attention and support, albeit that its occurrence has not plummeted. Not much by way of policies and protocols to insulate users from abusers have been designed, deployed and implemented. The capabilities of individuals, Organizations and to a large extent Government to identify and track cyber attackers is still relatively weak. And when abuse and harassment occur, not much in terms of mitigation measures are currently

in place to help those who suffer such abuses to cope, recover and maintain their sanity.

1.7 The guidelines are expected to be a foremost step towards having coordinated approach to address cyber menace and is not intended to be all-encompassing but are to be used along with the various Acts listed in Section 1.1 above.

2. Evolution of Online Abuse and Harassment in Ghana

2.1 The internet revolution became prominent in Ghana from 1995 after the Ministry of Communication registered the "ghana.com" in 1993. Prior to 1995, very little was known about the internet and its capacity to propel economic growth, enhance connectedness and bridge social gaps among all genders. Ghana has since made modest progress in the use of internet infrastructure as the economic fortunes of the country improve with time.

2.2 Ghana's online space is highly liberalized with many service providers, including the major telecommunication companies such as MTN Ghana, Vodafone Ghana, Globacom, Airtel Africa and Millicom Ghana. Currently, there are circa 8 million Ghanaians who have access to internet services. The mobile phone is a commonly used device to access online services in Ghana. The use of the mobile phone for internet services present the most significant cyber challenge to Ghana as there are a lot of vulnerabilities inherent in the mode.

2.3 Currently, there are no internet use censorship laws in Ghana. Governments do not monitor the activities of users of the various online services in Ghana. The constitution of the Republic guarantees freedom of speech and press, and this fits into why Government's would not want to censor activities of individuals or groups online.

2.4 Because online activities of individuals and groups are not monitored and the anonymity of the cyberspace, many citizens often suffered abuse for expressing their opinions. In recent times online abuse and harassment appear to increase as more people gets richer and are able to afford communication devices, and more people are becoming ICT literate. The increase in abuse is, therefore, explained by increased access to online services in Ghana.

3. Factors sustaining online abuse and harassment in Ghana

3.1 Absence of online abuse and harassment policies in Ghana has been a major concern to why abuse has become that rampant. Though the Criminal Code, 1960 (ACT 29) makes provision relating to threats, it is not sufficient to deal with sophisticated crimes such as those that happen online. The tracking of such crimes is a difficult task for many government agencies such as the police service. It is therefore essential to note that to prevent the rampant online abuses and harassment would require a dedicated policy designed for that purpose.

3.2 Misaligned incentives between internet users and abusers. The motivation for users and abusers differ, and since there are satisfaction and arbitrage in the exploitation of

the vulnerabilities in the internet system, abuse is unlikely to attenuate until the arbitrage is narrowed.

3.3 It is also essential that the Government addresses the lax mobile phone sim registration process in Ghana. It is undeniable that sim card registration in Ghana is not thorough and comprehensive enough to ensure that no person is able to do multiple registrations. It is also possible for people to acquire a sim card without the proper registration process. Such fraudulent sim cards are often used to open different social media accounts through which they abuse innocent citizens without a trace of them.

3.4 The other fact relates to the weak addressing system in Ghana. Prior to the recent introduction of the digital addressing system in Ghana, there were no elaborate addressing in place in Ghana. People were only required to provide a description of where they live in completing many documentations, including opening social media account. The weak addressing system has enabled and emboldened those using such information for their social media handles to abuse and harass others, knowing it will be challenging to track them.

3.5 Absence of a functioning national ID system. One setback militating against sanitizing the cyberspace has been the reason that people can participate in the cyber ecosystem by assuming a complete anonymity status. It suffices to mention that some platforms require users to sign up using a functioning e-mail ID and phone numbers. But the weak regulation of phone registration has made it easy and possible for anyone wanting to participate in the cyberspace to hide his/her true identity. Same challenges are faced in e-mail registration process.

3.6 Weak database system in Ghana. Ghana in recent times has embarked on a number of initiatives aimed at increasing the procurement of information of Ghanaians with the primary objective of fostering development and growth. These initiatives cover the digitalization programmes including the National ID Card System, digitalization of the office of Registrar General's Department, Digital Property Addressing System, Mobile Money Payment interoperability system, deployment of medical drones, and digital drivers' license. Though these are bold steps towards a digitized society, we still suffer fragmentation, weak linkage and connectedness between these systems. In most instances, the databases are standalone systems, and that is a challenge to building a comprehensive data system for the entirety of the country. We still do not have one "stop shop" where the various systems congregate.

4. Sanitization of the Cyber Space

4.1 Online surveillance – One key to sanitizing the cyber ecosystem to ensure users are safe and secured requires that various agencies with such responsibilities are resourced to conduct routine surveillance. The surveillance must take different forms, including monitoring, specialized studies, identify vulnerabilities swiftly and consistent evaluation of systems. Here, the services of ethical hackers are essential if

the authorities are to be on top of the issues of abuses in the ecosystem. Through the surveillance programme, and through the use algorithms one will identify the browsing history of users which then will serve as a guide to moderate users and prompt them when they go beyond their frequently accessed sites.

4.2 Establish protocols for internet use – the need to have standardized protocols to guide the conduct of users of internet services is critical. It is a truism that to police the internet is near impossibility. However, protocols for different users, including students, will define the operating fields for different segments of user categories. For instance, such a protocol should expand on the existing parental control measures to protect minors. It should also detail out measures such as having inbuilt prompters to seek user consent to sites considered expressive.

4.3 Enhance education- there is no doubt that the key to healthy cyber activities in Ghana is education. Ensuring that users are abreast with all the vulnerabilities that malicious individuals can exploit to abuse them is critical to sanitizing the cyberspace.

5. Target audience of the guidelines

5.1 The guideline is targeted at all users of the internet in Ghana. Three main actors identified in the cyber-ecosystem are a) Internet Users, b) Service Providers, and c) Cyber Attackers.

5.2 Internet users are sub-categorized into three groups, namely; Individuals, businesses, and the government. Individual users are those who use Personal Computers (PC) or mobile phones for personal businesses. They cover but not limited to educational, social and economic purposes. Individuals are more vulnerable to cyber threats. Many have little or no knowledge of information security and how to protect their activities on the internet. There are mostly no protocols for enforcement of cybersecurity awareness in many countries. The individual's investment in cyber education is linked to his understanding of the cyber environment. Also, the providers of the services that the individual uses often attempt at investing in their protection through contracting. Governments, in some instances, invest in cyberinfrastructure to protect users. When a cyber-disruption occurs, individual users often suffer both emotional, financial and reputational damages.

5.3 The next users are businesses – big companies, medium and small. Often, the use of the internet in the business environment follows specific rules and regulations though it is not a widespread phenomenon, especially for small and medium businesses. Investments in creating cybersecurity awareness are high, especially for businesses which rely on IT infrastructure for their activities and production. Despite the watchful eye, many businesses put on cybersecurity; they still are vulnerable and faces unabated cyber threats. Those who outsource their IT services are not free either since many of such companies do not have full prove systems which insulate them from cybercrimes.

5.4 The next is the government. Governments rely on IT infrastructure to deliver many social and economic services. In the areas of the provision of critical infrastructure and defense infrastructure services, governments use the internet extensively, thereby exposing them to cyber-risks. Many governments, especially those in the Western Worlds, invest significantly in protecting both critical and defense infrastructure. Also, many have well-developed protocols for the management of such infrastructure. Nevertheless, cyber threats are a common occurrence for both advanced and developing country governments as the incentive and motivation for hackers to attacks in many instances, outweighs the cost.

5.5 The IT service Providers category has as its primary function as finding solutions to cyberspace challenges. It remains the critical part of the system required to overcome cybercrimes, especially in developing countries where bureaucrats' capacity is weak. Generally, IT service providers demonstrate a higher understanding of the cyber challenges and continually works at evolving workable solutions for users alike. There are three main subcategories of service providers; the private IT firms, dedicated government IT Unit(s) and Research Institutions. The private IT firms dominate the market and are at the forefront of the provision of many novelties of solution products. Profit motives drive them, and their objectives do not necessarily meet those of the government. The dedicated government Unit(s) has also been a key component in finding and providing solutions to malicious cyber activities. In many instances, the core objective of government agencies is to provide security for government machinery and critical infrastructure. The research institutions are mainly interested in understanding the cyberspace via empirical research. Such empirical research becomes vital in the development of new cyber-products for the market. Though the three service providers have different objectives, their end goal remains the same- get ahead of the bad guys.

5.6 Attackers are those who conduct malicious activities to vitiate the benefits of the internet. They are adversaries who inflict havoc on internet user for varied reasons chiefly for monetary rewards. We have individual hackers, organization sponsored attackers as well as state-sanctioned attackers. Cyber attackers target users based on the level of user vulnerabilities, business interest and national interest (economic or military). Attacks are on ascendancy because of the high benefits to attackers and the low cost of such venture to them.

6. Methods used to course Online abuse

6.1 Internet abuse in Ghana takes varied forms, and different platforms are used. The first is **Cyberstalking:** It is when an individual sends numerous unsolicited messages to another person (i.e., "direct communications") that cause the other person distress, anxiety or other forms of harm. It also includes e-mailing or directly messaging a victim online; the practice of "tagging" or "@-mentioning" someone on social media

can be another means of "cyberstalking.". This activity can arise out of malice, obsession or fixation on the part of the perpetrator.

6.2 The second method of internet abuse is **Massaging**. Sending intimidating, threatening or offensive messages to a target audience. Online abuse can also take the form of grossly offensive, aggressive and threatening messages that put an individual in fear of her personal safety or security.

6.3 **Online impersonation and trolling:** It involves harmful messages and communications about a person sent to a third party rather than directly to the victim (i.e. "indirect communications"). These communications can subsequently come to the knowledge of the victim and cause anxiety, stress or fear. A typical instance is where people set up websites dedicated to monitoring and criticizing a journalist. And also the posting of (real or doctored) intimate images of the victim without the victim's consent (i.e. "revenge porn"), and the publication of fake profiles, photo-shopped headlines, and doctored social media posts aimed at destroying the credibility of the victim and subjecting her/him to abuse.

6.4 **Online harassment campaigns (including "pile on" harassment)**: It is where a person experiences a sustained campaign of harassment from a number of different individuals. This campaign may be coordinated, or it could occur without prior organization. For example, it can start with one message from one user that then provokes many other users to send offensive, violent, intimidating, hostile or targeted messages to the victim (i.e. "pile on").

6.5 **Doxing**: This is the online practice of researching and broadcasting private or personally identifiable information about an individual – such as her telephone number or e-mail and home address – in an environment that implies or encourages intimidation or threat.

7. Punishment for online offenders

7.1 To effectively address the breaches in the cyber ecosystem, Ghana needs to make cyber-attacks unattractive but removing the incentive for such deceitful acts. The first punishment for internet offenders is **BANS** and **PROBATIONS**. Anyone found to be perpetuating or promoting online abuse MUST be ban from participating or doing anything on that platform. Their accounts must be deactivated and suspended from joining any platform for a period of 3 months. Subsequent to their return after serving the ban, the activities of such people must be monitored and scrutinized to ensure they do not return to their old bad ways.

7.2 The next is **FINES**. Cyber-abusers must be made to pay a fine commensurate to the level of injury caused the abused. The quantification of the level of injury must be a function of the cost the abused suffer from the abuse. This must include material cost, emotional and mental cost and any other cost incurred by the abused. The fine must be paid within a month after the abuser has been identified and convicted of the crimes. Failure to pay the penalties, the individual, institution or state actor must

suffer prison sentence equivalent to the injury caused and be determined by a competent Court within the jurisdiction of Ghana.

7.3 The next is **CUSTODIAN SENTENCING** for cyber-abusers. Upon establishing that an abuse has occurred through a legal system, the abuser(s) must be made to suffer sufficient custodian sentencing for their crimes. The determination of form and duration of sentencing must be the privilege of the Courts.

8. Measures to enhance cyber hygiene

8.1 Establishment of a National Data Base of Cyber Abusers (NDBCA). There must be a national database of all cyber abusers and must be accessible to all agencies working in the cyber ecosystem, including CSOs. The compilation of such a list will aid the fight against internet abuse in Ghana. Through the use of data science algorithms, it is anticipated that cybersecurity agencies will be able to use such a database to trace those abusers, not in the list.

8.2 Streamline of the reporting systems in Ghana. To encourage those abused within the cyber-space to report abuses require that the reporting channels be streamlined. Physical reporting is encouraged, but the agencies of police and the CHRAJ must establish digital platforms through which people can report abuses. The platforms must be simple, accessible and tailor-made for Ghana's purpose.

8.3 Investigation of reported abuses. It is highly encouraged that reported cases of internet abuses must be promptly investigated and culprits brought to book. This requires that the police, as well as CHRAJ, must build capacity in the new frontiers of technology, innovation and data analysis to be able to take up reported case and investigate them speedily. These agencies can also rely on the expertise of CSOs where necessary.

8.4 Passage of necessary legislation(s) on cybersecurity. It is important to emphases that to effectively deal with cyber excesses require that the congenial legal environment must exist. To this end, it is a must that the Cybersecurity Law be passed, necessary operational manual developed to guide internet activities.

8.5 Deepen the international protocols on internet use. The internet is a global commodity, hence to effectively address the side-effects of such a product require global level efforts. Tech producers, global institutions as well as individual sovereign countries collaborate more in ensuring safer products are developed, safer use of such products and where user abuses are identified, concerted efforts are solicited for a sustainable redress.

8.6 Sustained education and campaign on cyber hygiene. It is critical that Ghana institutionalized cyber-hygiene systems in our education and teach students about such protocols. Campaigns that promote cyber-free and sanitized environment must also be encouraged and supported.

9. Forms of rehabilitation Support for the Abused

9.1 Those abused must be given some level of support to aid their swift rehabilitation, and these assistances can take any form. Below are some of the habitation support mechanisms:

- Emotional Support;
- Psychological support;
- Economic and financial aid;
- Infrastructure support; and
- Any other support mechanism with the capacity to aid speedier recovery.

10. Definitions

10.1 Cybersecurity- is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

10.2 Laws- refers to legal regimes promulgated in Ghana to guarantee the freedom of all Ghanaians in the cyber-ecosystem.

10.3 Internet Security - consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, e-mail addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

10.4 Cyber-Hygiene - refers to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

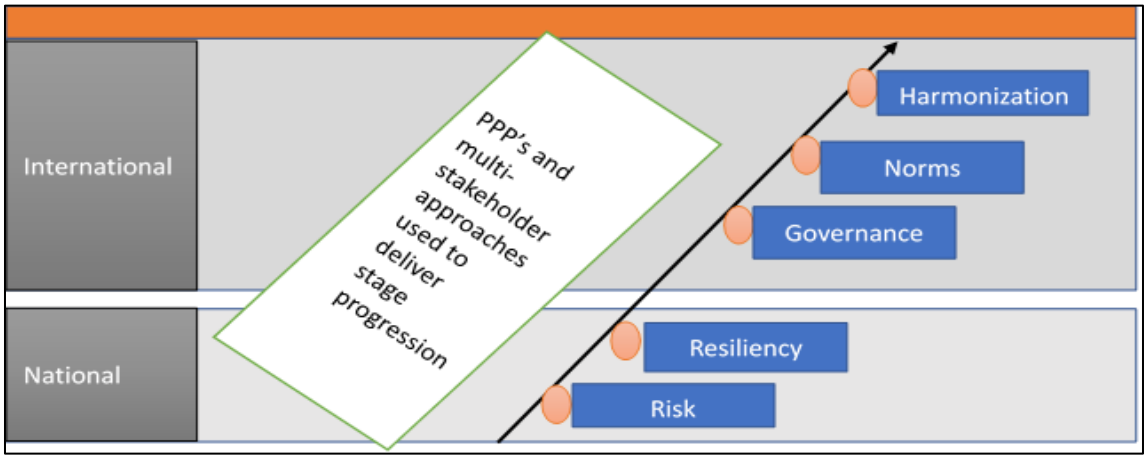
10.5 Cybersecurity Actors- refers to all people (internet users, IT companies, Government and cyber abusers) who in one way or the other participates in the ecosystem.

10.6 Cyber Abusers- refers to those who through malicious means inflict pain (emotional, financial, physical et al.) on others.

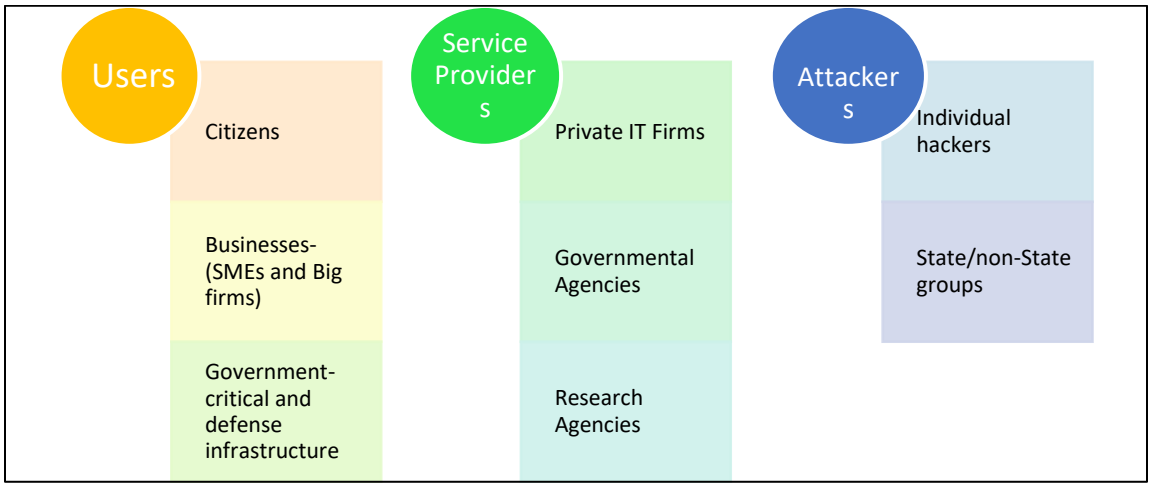
10.7 Cyber abused person- refers to those who suffer any form of pain as a result of malicious activities of crooked individuals through internet exploitation.

1. Appendix

1.1 Progression of Cybersecurity Policy



1.2 Key actors in the cyber ecosystem



1.3 Typography of Cyberspace

ACTORS	PURPOSE OF TECHNOLOGY USE	CYBER THREAT SOURCES	RISK EXPOSURE LEVEL	SOURCE OF INVESTMENT	POTENTIAL IMPACT OF CYBERATTACK	ISSUES/POLICY ENVIRONMENT
USERS						
Citizens	For social, educational and economic reasons	• Domestic • International	Moderate-high depending on knowledge on cybersecurity	• Individuals • Service providers • Government	• Emotional • Cost • Damaging	Citizens are an easy target due to the lax protection environment.
Businesses -SMEs -Big companies	Business development and social good	• Domestic • International	Moderate-high and depends on • The rate of internet use • The capital base of the business • Orientation on	• Businesses • Government (tax rebates, subsidies, training etc • R&D support	• Identity and business damage • System collapse • Brand insecurity • Financial stress	Businesses with large balance sheets are more secured relative to those with a weak balance sheet.

			cybersecurity • Policy environment			
Government Infrastructure -Defense -Critical -others	Security services and ensuring efficiency, quality and timeous delivery of public goods	• Domestic • International	Low-high and depends on • Importance in the community of nations • Global posture • Economic and political stature • Quality of Defense infrastructure	• Government • R&D	• Compromises government services • National security threatened • Financial cost	Rich nations with high investments in cybersecurity cope well with cyber risks. Institutional capacity constraints not perverse as poor countries
SERVICE PROVIDERS						
IT Firms	To evolve solutions to cyber threats	• Domestic • International	Low-moderate and depends on • Technical competence level	• Individual businesses	Slows technology innovation production Business collapse	IT firms are profi oriented and provid their services on when there is rent. The are not the mainstay finding a sustainab cyberspace soluti path.
Governmental Agencies	To understand security threats to government and citizens	• Domestic • International	Low-high and depends on the • Capacity of bureaucrats • The policy environment • Funding	• Government • R&D	Affects the protection of government and citizens	The government has th mandate of providi security for all, b human resourc inadequacy continues be inimical to th performance of th function aptly
Research agencies	To come out with empirical evidence and sustainable solution	• Domestic • International	Low-moderate and depends on • Funding adequacy • Competence of researchers	• Government • Private sector • R&D	Sustainable cyberspace knowledge production slows	Funding opportuniti are small and hav prevented RAs matching the fas changing phase cyberspace
THREAT SOURCE						
Individual hackers (domestic or international)	As a tool for conducting cyber crimes	States and companies attacked potentially could target such criminals	Low risk	Returns from attack	No impact. Unless there are attacked back.	The incentive for attac outweighs the cost and punishment. There is high energy on attackers' part to evol new attacking techniques.
External State/non-state actors	To disorganize other nations for varied reasons	Attacked States could retaliate	Low risk	Returns from attack	No impact. Unless there are attacked back.	Almost zero punishment for State attackers and that serves a great deal in their continual attackin activities