Cyberspace Improvised Explosive Device and the Failed State Catapult- The Strategic Symbiotic Relationship Failed State Status Offers Nation-State Cyberwarfare Arsenals

Denise N. Baken and Ioannis Mantzikos

HiCN Working Paper 166
January 2014

Abstract: Cyber technology has revolutionized communication in Africa, catapulting even the most destitute of the continent’s failed states into a global smorgasbord of choices never before imagined. Accessing these choices via mobile telephones and internet cafes, local inhabitants view their new found treasures through the poverty, unemployment and hunger that is pervasive to their right and to their left. Some have found an economic niche in this new technology, creating their own small businesses through internet crime. Success in this field has resulted in activities that generate 11% of the world’s cyber crime, even though they encompass only 6% of the total internet user population. Exploitation of the cyber highway has been facilitated by the failed states’ corruption and non-enforcement of international telecommunication union regulations and standards. They also represent a strategic opportunity for nation states developing cyber warfare arsenals. These purveyors of economic doom can provide countries inclined to expand their cyber warfare arsenals with the cyberspace equivalent of “improvised explosive devices,” the cyberspace equivalent of the menace that perplexed the West in Iraq and Afghanistan. Acting as front line foot soldiers they could bomb the target networks with niggling asset-demanding diversions while a more sophisticated and devastating attack is initiated. This paper investigates that possibility and the candidates who court fragile African nation-states with investments, aid and diplomatic recognition. Countries such as China, India and Iran have initiated cyber attacks from their own cyber borders. Initiation of attacks from failed state borders, by failed state mercenaries offers a robust cyber warfare attack tool these countries could readily incorporate into their arsenals.

1 Denise N. Baken, PhD, George Mason University, Fairfax, Va and University of Maryland University College, Adelphi, MD.
2 Ioannis Mantzikos, PhD Candidate, Kings College of London, London, UK
Introduction

The cyber arms industry is experiencing a tremendous boon. This ever expanding use of cyber space offers a means to successfully execute an intentional intrusion into a sovereign government’s cyber territory in order to procure national security information; information that would otherwise jeopardize relationships if obtained through alternate espionage channels. Spurred by the attacks on Estonia in 2007, South Korean in 2008, Israel in 2009 and Iran in 2010, the industry is well aware that the quickly advancing cyber arsenal technology is shaping a new approach to the Internet. The advancements are moving at a rate that exceeds the ability of policy makers to keep pace creating a sensitive situation for the diplomatic community. This was demonstrated when the Ghostnet attacks were publicized and China was accused of instigating the intrusion on 103 countries, accusations that continued for months, because of the nature of the targets of the intrusions and the location of the attacks’ origin, the University of Electronic Science and Technology of China. China denied any knowledge of the cyber breaches but the situation raised a serious military strategy-international diplomacy question: how does a nation-state execute attacks using this new arsenal without jeopardizing relationships with an ally or agreement partner?

One potential response is to initiate such attacks from inside the geographic/political borders of a third party cyber location. This permits anonymity and/or plausible deniability. The cyber space would function much as the current practice of prepositioning

---

3 Error! Reference source not found.
4 Error! Reference source not found.
5 Error! Reference source not found.
6 Error! Reference source not found.
troops and logistics at a forward base within an Ally’s territory. The cyber space within the borders of another country does not require a treaty and the arsenal utilized need not employ international travel papers. Attacks can be executed without the host country’s knowledge or support.

However to execute such attacks the Nation-state employing this tactic must ensure several criteria are met. Chief among these criteria is the possession of modern fiber-optic information communication infrastructure that meets International Telecommunications Union standards. This ensures all activities are transmitted quickly and reliably, improving the probability of success. Next it is important that the third party Nation-state have sufficient political distractors that careful ITU monitoring is less likely. This offers the attack execution high probability of anonymity because the third party Nation-state will not rigorously enforce information communication technology (ICT) regulations. This probability is important because it offers freedom of movement and tactic execution. A third criterion is that the Nation-state must have a readily available population whose value system is receptive to and had experience participating in cyber crime activities. This supports execution by experienced personnel and plausible deniability. Fourth, and just as important as the others is the criterion that the Nation-state reflect a economic environment that is conducive to choosing participation in these activities as a viable employment alternative. The Nation-states that most readily meet these criteria are the fragile or failed states of Africa’s Sahel region.

This paper investigates the hypothesis that the fragile/failed states of the Sahel represent a sufficient number of these criteria to fulfill the requirements of developed nations who are establishing and implementing cyber warfare strategy. It examines the exploitation potential of a sophisticated cyber highway under the governing policies of a failed state’s corruption and/or non-enforcement of international telecommunication union regulations and standards. Leaders within the region understand the need for controlling the information highway, but they lack the assets or the will, or both, to do so, leaving cybercriminals free reign.

7 Error! Reference source not found.
Background

In 2009 researchers from the Munk Center for International Studies at the University of Toronto uncovered a series of spyware monitors on computers owned by the Dalai Lama, NATO, the Embassies of India and Pakistan. In all, more than 1200 computers in 103 countries had been surreptitiously tapped and examined for information of interest to the perpetrator or the perpetrator’s “client.”

When identified, the perpetrator was a young researcher and well-known hacker from the University of Electronic Science and Technology of China. The investigators into the event did not attribute the effort to the government of China but the event begs the question could a nation-state successfully perpetrate a cyber event from a developing country without investigators being able to positively attribute the event to that nation? According to Rafal Rohozinski, one of the investigators of Ghostnet, there is every possibility that could happen. Rohozinski suggests outsourcing is a very viable alternative because it offers nations anonymity, saves international relations and leverages available local resources for event execution.

That local talent pool, as defined by the 2009 European Report on Development: Overcoming the Fragility of Africa, reflects the cyber terrain’s future demographic: one that is young, talented, in a developing nation, and in possession of a personal value system that justifies participation or instigating such acts. These locations also boast corrupt authorities or those without the will or the resources to pursue such activity. If you are governing where there is civil unrest or lack of services, cyber crime is not your highest priority.

These proposed and new telecommunications systems create an environment for cyber crime prosperity, they also offer opportunity for organizations to exploit the paucity of administrative process that currently exists in many of the failed and fragile nations that could benefit. This same scenario existed in 1989 when Romania emerged from its
revolution. Enthusiasm for the opportunities that lay ahead was high. However, conditions were not conducive to immediate prosperity. The compromised infrastructure and poor economic policies and decisions caused Romania to fall behind its neighboring Balkan states. In an effort to compete with the surrounding more developed countries, Romania initiated a strong telecommunications infrastructure. In 1995 the country embarked on an Internet growth effort that would move it from its non-competitive lowest Internet penetration to one of dynamic competitiveness.\textsuperscript{12} In 1995 the gross number of Internet users lagged its Central and Eastern European neighbors. It didn’t even register against Western countries.\textsuperscript{13}

By 1999, it experienced an exponential growth that averaged 28% a year when the average was 22%. Rural Romania had automatic switching stations for over 90% of the population and the mobile market was the most active of the options available.\textsuperscript{14}

By 2010, the number of Internet users had risen from a low of 3.6% in 2000 to 35.5%.\textsuperscript{15} The broadband offerings and documented speed of data transmission exceeded that of its more developed European Union counterparts.\textsuperscript{16} In January 2011, WIRED Magazine reported that Romania had another Internet distinction. Its little town of Râmnicu Vâlcea was the cyber crime capital of the world.

The article outlined the economic impact cyber crime was having on the area, the economy and the people with the list of cars, homes and specialty shops the small area can boast. This little town of 120,000 came to depend on income from cyber crime when it found no other way to economically rebound from the 1989 abrupt change in government after the people’s revolution. The people struggled for nearly 10 years; then, when the Internet became a part of their lives, many of the young people stumbled upon online scams and the profits they derive.\textsuperscript{17} Since then the town’s people have never looked back. Particularly

\begin{itemize}
\item \textsuperscript{12} Error! Reference source not found.
\item \textsuperscript{13} Error! Reference source not found.
\item \textsuperscript{14} Error! Reference source not found.
\item \textsuperscript{15} Error! Reference source not found.
\item \textsuperscript{16} Error! Reference source not found.
\item \textsuperscript{17} Error! Reference source not found.
\end{itemize}
poignant was the ethical dilemma the young men and women in town face when they cannot find a job locally doing anything else that pays as well. 18

Romania, a former Soviet Union country of 22 million has one of the best communication technology infrastructures in the world. Download speed is faster than the United States, Canada and the United Kingdom. Its flourishing mobile market has four 3G licensed services, a CDMA operator and fixed lined cable capability. All of this cyber market support has been a boon to the organized crime syndicates who have coopted cyber terrain for their own profit. One of the reasons for the flourishing industry’s success is lack of enforcement.19 This has changed with recent arrests of leading criminal group members.20 In the last few years Romania has worked with the United States to curb Internet criminal business ventures with combined arrests in 2010 and 2011 surpassing 1500 cases. One raid alone in 2011 resulted in arrests of over 100 suspects.

Moldova, also a haven for organized cyber crime, had only 12% of its attacks prosecuted in 2007.21 Activities from money laundering to credit card fraud are now being prosecuted with 2010 seeing Moldova’s Center for Economic Crimes and Corruption arrest 12 of its most prominent fraudulent crime perpetrators.22

Previous safe havens are no longer safe. This attention from the authorities has caused cyber crime bosses to look elsewhere to continue their profitable businesses. That elsewhere could be in one, or more, of the fragile or failed states of Africa.

Russia used organized cyber groups such as these to conduct denial of service attacks against the country of Georgia in 2009.23 Leveraging the capabilities within this specialized crime community, Russia executed a denial of service attack that simply overburdened the Georgia system with page requests from a network of infected machines programmed to direct their page requests at a specified target. It was a tailored attack,
executed by Russian cyber criminals.24

Criteria

*Possession of modern fiber-optic information communication infrastructure*

In January 2012, IT News Africa reported that over the last 10 years Africa experienced a 2,000 percent increase in Internet use. This compares to a 480 percent growth everywhere else in the world.25 This growth was attributed to the tremendous telecommunications access improvements the people have enjoyed in that same 10-year period.

For, while the overall number of users is small, the percentage of change increase per year is astounding. (Figure 1)
<table>
<thead>
<tr>
<th></th>
<th>Benin</th>
<th>Burkina Faso</th>
<th>Cameroon</th>
<th>Chad</th>
<th>Mali</th>
<th>Mauritania</th>
<th>Niger</th>
<th>Nigeria</th>
<th>Total</th>
<th>Rate of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50</td>
<td>25</td>
<td>60</td>
<td>15</td>
<td>25</td>
<td>10</td>
<td>15</td>
<td>420</td>
<td>620</td>
<td>71%</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>48</td>
<td>100</td>
<td>30</td>
<td>35</td>
<td>12</td>
<td>19</td>
<td>750</td>
<td>1064</td>
<td>107%</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>53</td>
<td>170</td>
<td>35</td>
<td>50</td>
<td>14</td>
<td>24</td>
<td>1769</td>
<td>2205</td>
<td>152%</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>65</td>
<td>250</td>
<td>40</td>
<td>60</td>
<td>20</td>
<td>29</td>
<td>50000</td>
<td>5564</td>
<td>57.5%</td>
</tr>
<tr>
<td></td>
<td>125</td>
<td>90</td>
<td>330</td>
<td>60</td>
<td>88</td>
<td>30</td>
<td>40</td>
<td>8000</td>
<td>8763</td>
<td>26.6%</td>
</tr>
<tr>
<td></td>
<td>150</td>
<td>110</td>
<td>548</td>
<td>90</td>
<td>100</td>
<td>45</td>
<td>55</td>
<td>10000</td>
<td>11098</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>160</td>
<td>140</td>
<td>---</td>
<td>130</td>
<td>125</td>
<td>--</td>
<td>80</td>
<td>11000</td>
<td>11635</td>
<td></td>
</tr>
</tbody>
</table>

Source: Statistical Yearbook, Fifty-third Issue: Data Available as of Oct. 2009^26

Figure 1. Internet Usage 2002-2008^27

The proliferation of wireless access has connected even the most rural residents of Uganda, Mali or the Sudan to the rest of the world through Youtube, Facebook, email, e-commerce, and on-line banking. It is set to aid healthcare through telemedicine and improve even the remotest citizens’ quality of life through opportunities like online education. Technology is expected to continue to improve life as infrastructure improvements such as the 2009 fiber-optic submarine cable system project Seacom that linked Mozambique, Tanzania, Kenya and South Africa to Europe and Asia continue as expected. There has

---

^26 Error! Reference source not found.  
^27 Error! Reference source not found.  
^28 Error! Reference source not found.  
^29 Error! Reference source not found.  
^30 Error! Reference source not found.
already been Eassy, a 2010 Eastern Africa cable system and Wacs, a Western Africa cable system, that started just this year. All of these should compliment the recently announced BRICS project that will link Brazil, Russia, India, China and South Africa (BRICS) to the United States. Projected for a 2014 completion, this private investment effort will increase connectivity both within the continent as well as outside. Together, these economy-boosting projects should fill the technology gap that limited development in the region and improve the attractiveness of Africa as a foreign direct investment target.

*Nation-state has sufficient political distractors*

The Sahel has the same political and economic landscape reflected in the wider region of Northern Africa. They have a population with a wide variety of, cultural backgrounds. Endowed with significant natural resources, these African countries share some of the world’s lowest standards of living. There is exploitation of these natural resources but corruption and direct flouting the law by government officials has caused massive unemployment, little foreign direct investment and a growing informal financial sector this informal market has already created space for money laundering, computer bank fraud, and identity theft.

*Nation-state must have a readily available population with receptive value system is receptive*

Africa’s attractiveness benefits from the fact that, by the year 2040, 20% of the world’s pool young people will reside in this region along with half of the world’s employable population. Nigeria, for example has one of the most experienced cyber crime cadre in the field, the Yahoo boys, a group known for their preference for Yahoo’s users, its chat rooms and email access. According to a recent descriptive study of the Yahoo boys, the young men are between 22 and 29, they are university educated, as are their parents.
However, the medium family monthly income is between 25,000 and 30,000 Naira, equivalent to roughly 160 US dollars and many of the perpetrators are unemployed. In addition, the Vice Chancellor of Osun State University recently stated that the computer science students were focused on graduating to make money in cyber crime. This indicates a ready pool of highly educated perpetrators is available to execute attacks. Currently the nation exercises minimal information communications technology (ICT) oversight and the students know and understand the implications of this fact. These perpetrators are within the cyber warfare perpetrator’s demographic and could train large numbers of recruits in the same successful practices.

*Nation-state economic environment conducive to cyber crime activities*

Using the Sahel as the location for illegal activity has precedent. The Northern African region that encompasses Senegal, Mauritania, Mali, Niger, Chad, Burkina Faso, Benin, the Sudan, and the northern parts of Nigeria and Cameroon are already used as one with a seamless borders by terrorist groups and organized crime. They execute attacks freely conducting business without impediment. These business endeavors exploit the lack of controls and demonstrate an opportunistic approach to their circumstances. These states are severely hampered by almost nonexistent financial resources, limited advanced technology and, often, graft and corruption. As a result both groups function within the protection of a failed state’s weaknesses.
Thus far we have identified the conditions for and impact of cyber crime as an entity separate from cyber warfare. But the reality is tremendously talented cyber activists can, and will, mesh cyber crime and cyber warfare to commit computer fraud or attack vulnerable information community infrastructure, all to further their stated goals. Even Al Qaeda demonstrated a desire to enter this market when they tried recruiting former Soviet-bloc computer science professors with the hope of sending them to Africa to initiate attacks against the United States before 2005.\textsuperscript{42} Indications are that they ceased this approach by 2007, when they allegedly found takers.\textsuperscript{43} There are no indications they stopped all together any attempts to secure the talent.

\textit{Exploitation potential of a sophisticated cyber highway}

\textsuperscript{40} Error! Reference source not found.\textsuperscript{41} Error! Reference source not found.\textsuperscript{42} Error! Reference source not found.\textsuperscript{43} Error! Reference source not found.
What if Ghostnet’s perpetrator had initiated the intrusions from one of the Sahel states, where even geographic borders have no real monitoring; and the region’s relatively small overall Internet presence has even fewer regulations and standards. Even in developed regions, law enforcement has difficulty keeping pace with cyber technology advancements. For authorities responsible for the Sahel’s cyber space control, this crime category’s relative importance may not warrant diligent supervision. This means that for extended periods of time, crimes will remain undetected or unreported. As Internet crimes increase in the region and/or trading partners object, enforcement may become more significant. At that point political will would offer impetus for change.

In 2011 the Financial Times reported that the cyber war industrial complex has evolved to accommodate the growing market. Perpetrators have recognized that, it is simpler, and less resource intensive, to execute attacks from the anonymity of the cyber terrain; increasing that anonymity by executing such attacks from a server located in the physical terrain of failed state locations improves the chances for continued activity. The nations seeking to develop Africa’s cyber infrastructure improvements are aware that this area is home to a burgeoning cyber growth market and the third largest percentage of cyber crime perpetrators.

The Sahel Cyber Crime-Cyber Warfare Environment

Nation-states executing a national security driven cyber warfare strategy may prefer to initially use local talent for the niggling attacks that coopt target nation resources and distract them from a larger more deleterious attack. Using the improvised explosive device of Iraq and Afghanistan as the model, these “niggling” attacks will cause damage that cumulatively becomes a significant concern to the target nation. They will be as extensive as the perpetrator nation needs or desires. The low cost of the readily available workforce offers Nation-states an excellent cost benefit ratio.

44 Error! Reference source not found.
45 Error! Reference source not found.
Adapting a ratio suggested by Kshetri:

\[
\text{Investment} + \text{Probability of Authority Intervention} = +/- \text{ Return on Investment (Profit/Loss)}^{46}
\]

Attacks such as these can be executed by local personnel. Uniform hacker software setup can be acquired for as little as $250 to $500. Yahoo boys could assist with the crimes committed or execute them directly. For instance the young men already know how to develop a relationship with security and bank personnel. They have developed local, national and international networks that nation-states could leverage to their own advantage. Any participants included in this activity would continue to enjoy social acceptance, as cyber crime is a highly practiced endeavor by both men and women. There is also the workforce that emerges with each University graduating class, individuals who have already expressed an interest in entering the cyber crime industry.

**Return on Investment**

The return on investment can be very high. In 2009 authorities estimated US internet losses at 240 million dollars \(^{47}\). Nigeria’s Muhammed Rudman, Chief Executive of the Nigeria Internet Exchange Point indicated that worldwide total was 114 billion dollars. Many of the schemes originated in Nigeria taking various forms to increase chance of success. There is also high return on investment probability in money laundering schemes using stolen credit cards to finance gambling play and later allocating the winnings toward terror attacks financing \(^{48}\)

**Probability of Authorities Intervening**

It is important to recognize that the success of this hypothesis is contingent minimal intervention from ICT regulators. The Sahel and its surrounding countries have long...
recognized the need for and the enforcement of more stringent ICT controls for its ever growing internet populations. However, thus far, the region has failed to adopt cohesive cyber crime laws or enact a standard similar to the Convention on Cybercrime of the Council of Europe.

<table>
<thead>
<tr>
<th>Country</th>
<th>ITU-R</th>
<th>ITU-T</th>
<th>ITU-D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burkina Faso</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cameroon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mali</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mauritania</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Niger</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senegal</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Source: ITU Global Directory as of 3 April 2012

Figure 3. International Telecommunication Union Standards

Initially ICT controls were deemed low priority because the total number of Internet users in the region were not significant. But the increased usage and the cyber crime already perpetrated from the region continues to make the controls an area of interest. The nation-states in the Sahel, however, do not have the assets to focus on or enforce cyber controls. The Organization for Economic Co-operation and Development (OECD’s) Financial Action Task Force recognized the lack of oversight and increased presence of criminal groups. This presence has created a strong shadow economy with an unregulated exchange of goods and services. This informal economic system has impeded the governments ability to acquire tax revenue, leaving it with insufficient funding to execute its responsibilities.

49 Error! Reference source not found.
50 Error! Reference source not found.
Each of the countries has Economic Community of West African States (ECOWAS) concerns that address challenges for transportation, utilities and information communication. The transportation requires upgrades to improve railway and port operations and replace aging air fleets. Electrical power needs improvements and information communication must undergo upgrades to improve regional integration capabilities. These upgrades/improvements have associated costs in the hundreds of millions of dollars, monies these counties do not have. These funding shortages impact the size of the military. The result is the Sahel has miles of border with little or no surveillance. Reports of corruption and graft are rampant in the area and that undermines public confidence and puts the people in the untenable position of trying to make a broken system work.

The lack of infrastructure and the accompanying public official corruption act as deterrents for investors, tourists and international businesses. These shortcomings have such a negative impact that the region as a whole is represented high on the failed state index (Figure 4).

<table>
<thead>
<tr>
<th>Country</th>
<th>Failed State Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chad</td>
<td>2</td>
</tr>
<tr>
<td>Mali</td>
<td>77</td>
</tr>
<tr>
<td>Mauritania</td>
<td>42</td>
</tr>
<tr>
<td>Niger</td>
<td>15</td>
</tr>
<tr>
<td>Adjacent states</td>
<td></td>
</tr>
<tr>
<td>Benin</td>
<td>74</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>37</td>
</tr>
<tr>
<td>Cameroon</td>
<td>24</td>
</tr>
<tr>
<td>Nigeria</td>
<td>14</td>
</tr>
</tbody>
</table>
These same characteristics make it attractive to individuals and groups who want to function without significant government interference. This is exactly what makes the region attractive to terrorist groups and other criminal organizations that would exploit the lack of oversight.

These conditions create an environment that supports continuance of the status quo and encourages opportunists to provide support services for this anonymous clientele. One example already exists, their Internet service providers who cater to these clients who seek to remain anonymous. The lack of strong information highway regulatory legislation appears to condone the situation.

It is these very conditions that make Sahel an excellent candidate for Nation-states to exploit for cyber attack.

**Conclusion**

Incorporating niggling cyber attacks into a Nation-state’s repertoire of weapons against the West reduces its attack footprint. Adding this new weapon, the sovereignties still achieve their goals and objectives. But they redefine the cyber crime committed so that it becomes a tool in the arsenal employed to achieve national security goals. Each act against an individual or financial institution would still represent a crime against state law. But both the Nation-state and the perpetrators have an ethical response that reconciles the act within each one’s own value system.

Cyberspace expands nation-states ability to inflict damage. Harm is inflicted on individuals or government entities as determined by the goals and objectives of the Nation-state. Impact can be significant and financial burden may exceed that of the attack of September

---

* Figure 4. Sahel States Failed State Position*[^52]

[^51]: 2011 Failed State Index
[^52]: Error! Reference source not found.
11, 2001. Maintaining a presence on the web is critical to any organization seeking to market its skills and ideology. The targets may not feel withdrawal from the Internet is an option thus making the pool of available targets almost constant.

There is also the benefit to the fragile African nation-states of investments, aid and diplomatic recognition. Countries such as China, India and Iran have initiated cyber attacks from their own cyber borders. Initiation of attacks from failed state borders, by failed state mercenaries offers a robust cyber warfare attack tool these countries could readily incorporate into their arsenals.

BIBLIOGRAPHY

Error! Reference source not found.