Structure of Presentation

- What is “Cyberspace” and Why Does it Matter?
- Africa’s Cyber Threat Landscape
- Implications for Security Actors
Evolutions in Communications and Firearms Technologies

Timeline of Evolutions in...

**Firearms:**
- **Matchlock Rifle**: 1570s
- **Flintlock Pistol**: 1750
- **Gatling Gun**: 1865
- **M16**: 1969
- **Computer-Assisted Firearm**: 2013

**Communications Technology:**
- **Telegraph**: 1838
- **Computer**: 1945
- **World Wide Web**: 1991
- **iPhone**: 2007
- **Military Drone Swarms**: 2021
Defining Cyberspace

Information Security

INFORMATION OPERATIONS

IMPROVISED EXPLOSIVE DEVICES

OPEN SOURCE INTELLIGENCE

Cyber-enabled threats

Cybersecurity

Confidentiality

CIA Triad

Integrity

Access
Africa’s Evolving Cyber Threats

Figure 5: Cyber Threat Framework and African Cases

<table>
<thead>
<tr>
<th>Threat</th>
<th>Definition</th>
<th>Cases Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organized Crime</td>
<td>Criminal enterprises that profit from illicit activities through cyber-enabled means.</td>
<td>Silver Terrier Business Email Compromise Network</td>
</tr>
<tr>
<td>Critical Infrastructure Sabotage</td>
<td>Attempts to weaken or destroy national, government or military infrastructure, hardware, or systems.</td>
<td>Horus Group’s Cyberattack Against Ethiopia</td>
</tr>
<tr>
<td>Espionage</td>
<td>Attempts to penetrate a system for the purposes of extracting sensitive or protected information.</td>
<td>China's Attack on the African Union</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pegasus Malware</td>
</tr>
<tr>
<td>Armed Conflict Innovation</td>
<td>The use of cyber-enabled technology to facilitate organized violence through changes in external communications, international organization, and combat operations.</td>
<td>Libyan Drone War</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Al-Shabaab and Twitter</td>
</tr>
<tr>
<td>Disinformation</td>
<td>Intentional dissemination of false information with the intent of advancing a political objective</td>
<td>Russian Disinformation and Troll Farming Campaigns</td>
</tr>
</tbody>
</table>
Threat 1: Organized Crime

How missed ‘red flags’ helped Nigerian fraud ring ‘Scattered Canary’ bilk Washington’s unemployment system amid crisis

May 24, 2020 at 6:00 am | Updated June 4, 2020 at 6:18 pm

By Jim Brunner, Paul Roberts and Patrick May
Seattle Times staff reporters

Threat 2: Critical Infrastructure Sabotage

BREAKING #TransnetHack I’ve been reliably informed that Transnet systems have been hacked. All employees received this communication to shutdown all laptop and desktops and not to access their emails.

#eNCA

Also DO NOT access emails on your phones until further notice.

No MS Teams meetings until further notice

Good Morning All. Urgent message from ICTM. Transnet systems have been hacked and compromised. Please disconnect from the Transnet network immediately until advised otherwise. This impacts remote access via APN/VPN (3g or home Wifi) or direct access via LAN if you are in the office. This will also include

Source: Bloomberg/Getty Images
Threat 3: Cyber Espionage

Infections, users, and cross-border targets of Pegasus malware in Africa.

Source: Reporting and data compiled from Citizens Lab and the Pegasus Project.
Threat 4: Armed Conflict Innovation

HSM Press Office @HSM_PR
Here are 2 of the Mujahideen inside #Westgate mall, unruffled and strolling around the mall in such sangfroid manner
pic.twitter.com/bMG87AQ0on

HSM Press Office @HSM_PR
The hostages who were being held by the Mujahideen inside #Westgate are still alive, looking quite disconcerted but, nevertheless, alive

HSM Press Office @HSM_PR
The incoherent ramblings of Kenyan officials and the blatant discrepancies with regards to the Mujahideen at #Westgate betrays their fears

Threat 5: Disinformation

Disinformation Campaigns in Africa

- 1 campaign
- 2 campaigns
- 3 or more campaigns
- Russian sponsored campaign(s)
Implications for Security Actors

- Threats are likely to accelerate
- Unconventional threats require unconventional solutions
- Africa at a critical juncture