Dark Consequences: How New Laws are Impacting the Cyber Threat Landscape

Charity Wright
Cyber Threat Intelligence Analyst
IntSights Cyber Intelligence
@CharityW4CTI
Back to the Future: APAC 2019

- Vietnam, China, Russia, Australia: Internet laws around the world, especially in APAC are creating lasting and permanent changes in the Cyber Threat Landscape.
- Nations are isolating their internet blocks and their citizens from access to the globalized internet.
- Isolationism, restrictions, and data privacy laws will drive citizens to the deep and dark web for anonymity, cryptocurrency, and access to otherwise inaccessible information, including crime.
Blast From the Past: The Internet

1960’s: World Wide Web theory as “ARPAnet”
1983: Internet is reality
1983: DNS System created
1985: Symbolics.com is first registered domain
1987: Cisco ships first router
1990: HTML created
1991: Internet goes public!
1997: Russian dark web emerges with hackzone.ru
2000: Cybercrime and hacking becomes big business with carder.org
Vietnam’s premier hacking group ramps up targeting of global car companies

Iran Launches New Military Command And Control Unit To Withstand U.S. Cyberattack

The New York Times

U.S. Escalates Online Attacks on Russia’s Power Grid
Bending the Internet: How Governments Control the Flow of Information

Net Neutrality Is about Government Control of the Internet
Around APAC in 30 Minutes:

Vietnam, China, Russia, Australia
Vietnam Cyber Landscape:

- Early 2000’s – Internet arrives
- Late 2000’s – Dark web activity begins
- Half of the country’s population of 93 million now actively uses the internet
New Internet Laws: Cybersecurity Law of 2018

- June 2018 - Vietnamese National Assembly passed a new cybersecurity law requiring tech companies to open offices in Vietnam, store local user data in Vietnam, and hand over any information the government requests.

- The law also enforces censorship of social media, with which internet companies have one year to comply.

- As part of the government’s censorship initiative, it created a cyber offensive unit of 10,000 members called “Force 47” to combat proliferation of views it deems inappropriate or toxic.
Vietnam’s Cybersecurity Law of 2018: Implications

- Force 47 frequently requests removal of social media posts that oppose the government’s views, threatening to block all internet users from accessing those platforms entirely.
- Social media giants and tech companies are forced to decide between censorship.
- Observed increase in Vietnamese-language internet traffic and activity on the deep and dark web.
- Thousands of users are migrating to Vietnamese-language forums to seek information on technology, cryptocurrencies, and cybercrime opportunities.
- RISK: Foreign companies operating inside Vietnam forced to weigh risks/benefits.
Vietnamese Dark Web Observations:

March 2019 – Increase in dark web usership on Vietnamese sites observed

![Graph showing membership growth over time](image-url)
Vietnamese Dark Web Observations:

Total Posts

<table>
<thead>
<tr>
<th></th>
<th>Mar-19</th>
<th>Apr-19</th>
<th>May-19</th>
<th>Jun-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Posts</td>
<td>811</td>
<td>828</td>
<td>834</td>
<td>842</td>
</tr>
</tbody>
</table>

IN THOUSANDS
Vietnamese Dark Web Observations:

Daily Logins

<table>
<thead>
<tr>
<th>Mar-19</th>
<th>Apr-19</th>
<th>May-19</th>
<th>Jun-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>650</td>
<td>662</td>
<td>675</td>
<td>685</td>
</tr>
</tbody>
</table>

AXIS TITLE
"If you open the window, both fresh air and flies will be blown in."
China Cyber Landscape

• 2018: China’s Internet population reached more than 772 million users
• 55.8% of population, exceeding the global average of 51.7%
• Internet Sovereignty
• Strictest internet laws of any single government in the world

• Huge strides in AI being used to monitor and track data
• Most expansive “surveillance state” in existence and history
• Recently began requiring tourists to download data-monitoring apps on personal phones
New Internet Laws: Cybersecurity Legislation of China

- 1997 CL97: First cyber crime law created
- 2003 Golden Shield Project, Great Firewall
- June 1, 2017 – Cybersecurity Law enacted
- June 2019 – Supplemented with the "Data Security Administrative Measures"
- Requires network operators to provide data under their control upon request
China’s Cybersecurity Laws & Surveillance: Implications

• Penalties: Network operators that violate the measures may be subject to public exposure, confiscation of illegal gains, suspension or a shut-down of their business, disabling of their website or the revocation of relevant business permits or licenses.

• Crimes will be investigated and punished in accordance with relevant criminal law.

• Recruitment of cyber-savvy tech generation to work for state

• RISK: Foreign firms inside China
Dark Implications: Evasion and Enforcement

• 2008 “Operation Tomorrow”, spurred “black web bars” used by youth
• Circumvention is possible
• Chinese are more active on the clear net because the government limits access to the dark web
• Cybercriminals use crypto language to hide true meanings of criminal behavior on clear web
Russia’s Cyber Landscape:

- 76% of citizens are using the internet (higher than South America at 73%, Southeast Asia at 63%, or Oceania at 69%)
- 109.6 million internet users in Russia
- 68% use desktops or laptops
- 61% use smartphones
- 85% of internet users in Russia access the web every day
- 6h29m daily internet usage
- 64% of Russians use the mobile internet
- 6 of the 10 most frequently visited websites belong to Russian companies
Russia’s Social Media Landscape:

- 49% Internet users in Russia use social media
- 70 million active social media users in Russia
- Most active platforms: YouTube, VK, and WhatsApp
- 83% of Russians use Vkontakte instead of Facebook (39%)
Legal Precedents in Russia:

- SORM, April 2014
- Data Localization Law, Sep 2015
- Yarovaya Anti-Terrorism Law
- VPNs and Anonymizers Law, Nov 2017
- Messenger Identification Law, May 2019
Russia’s New Internet Law: Sovereign Internet Bill

- Signed into law by President Putin on May 1, 2019
- Russian stance:
  - Designed to protect its network from foreign intervention
  - Prevent foreign intervention that might intend to disconnect Russia from the world wide web
  - Establishes a means for closure of Russian access to the internet while maintaining a functional internet inside their own borders
  - Russia states if they are cut off from the WWW, they could willfully disconnect from global root name servers, ensuring autonomous operation of RUNet, the Russian internet sector
Russia’s Internet Laws: Implications

- Specialized hardware and software installed in every Russian ISP
- Government and law enforcement have on-demand access to private data of citizens without subpoena or court order
- Russia can disconnect citizens from the world wide web
- Restrict internet freedom for users
- Bolster government grip on the internet used within its borders
Russian Dark Web Landscape
Russian Dark Web Rule #1: Never Target CIS/Russia

A post describing the arrest of a Russian hacker who tried to hack a local government site.
What’s Next in Russia?

- Dark web users will have to invest more time and thought into building proxies and anonymizing their infrastructures.
- Use of VPN companies that are compliant with Russian laws and passing information to government agencies (or not).
- Prediction: Creation of methods to bypass government inspection equipment or create alternative means of networking.
Australia Cyber Landscape: Internet Usership

- 88 percent were active users
- 14.7 million internet subscribers in Australia
- 69% of the population are active social media users
- 78% are mobile device users
- Fastest mobile device usership growth at 7% annual growth
Australia Cyber Landscape: Social Media Usage

**MOST ACTIVE SOCIAL MEDIA PLATFORMS**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Social Network</th>
<th>Messenger/Chat App/VOIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>YouTube</td>
<td>68%</td>
<td></td>
</tr>
<tr>
<td>FB Messenger</td>
<td>49%</td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td>34%</td>
<td></td>
</tr>
<tr>
<td>WhatsApp</td>
<td>22%</td>
<td></td>
</tr>
<tr>
<td>Snapchat</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Pinterest</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Google+</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Reddit</td>
<td>10%</td>
<td></td>
</tr>
</tbody>
</table>

**Survey-based data: Figures represent users' own claimed/reported activity.**
Australia’s Internet Laws: Telecommunications and Other Legislation (Assistance and Access) Bill

- Will allow Australia’s intelligence and law enforcement agencies to demand access to end-to-end encrypted digital communications
- Allows officials to approach specific individuals with demands, rather than institutions. Ex: Can force an engineer or IT admin to undermine security
- Companies that refuse or fail face fines up to $7.3 million; individuals face prison time
- Tailored access to individual programs could be a possibility
Australia’s Internet Laws: Implications

- Backdoors built into a product are accessible equally to governments and threat actors. Vulnerable to criminals and other state-sponsored threat groups.
- Companies might opt to turn off end-to-end encryption, disable smartphone “kill switches”, or take away users’ sole ability to decrypt their own smartphones.
- Draconian punishments set back human rights
- Backdoor-friendly legislation is the logical extreme, leading countries to block access to technology that offers robust security
Australia’s Dark Web Landscape:

1. Illegal drugs: Meth, MDMA, Cocaine, Mushrooms
2. “Medicare Machine”: Medicare and Medical Records
3. Fake ID’s, fraudulent documents
Global Implications
Global Implications: Business Data at Risk

- Handing over data to a foreign government
- Handing over access to your crown jewels to a foreign or domestic government
- Disclosures to your partners, customers, employees
- Increase in data storage to accommodate government requirements
Global Implications: Driving Citizens Underground

- Discovery: Young, technical generations in APAC countries are migrating to Deep and Dark Web (DDW)
- Purpose:
  - Anonymity
  - Financial Opportunities
  - Cryptocurrency Usage
Global Implications: Anonymizers

- Migration to cryptocurrency
  - Anonymous money-making opportunities
  - No tracking of income by government
- Anonymizers such as TOR and VPNs:
  - Help hide IP addresses and locations of logins
  - TOR used for dark web access to .onion sites
  - Hide web traffic from government surveillance
Internet laws around the world, especially in APAC are creating lasting and permanent changes in the Cyber Threat Landscape.

Isolationism, restrictions, and data privacy laws will drive citizens to the deep and dark web for anonymity, cryptocurrency, and access to otherwise inaccessible information, including crime.

Summary

- Vietnam: Cybersecurity Law of 2018
- China:
  - Cybersecurity Law of 2017
  - Data Security Administrative Measures of 2019
- Russia: Sovereign Internet Bill of 2018
- Australia: Telecommunications “Assistance and Access” Bill of 2018
What Can We DO About This?

- Use **Cyber Threat Intelligence** to conduct a **RISK ASSESSMENT**
- Know your **DIGITAL FOOTPRINT**: Understand the risk that your organization is already facing
- Know your **THIRD PARTY RISK**-- who has access to your data or traffic?
Contact: Charity Wright

Charity.wright@intsights.com
Phone: 808-258-2147
Twitter: @CharityW4CTI