

INTELLIGENCE

OSINT and Geopolitical Analysis

INFORMATION VS. INTELLIGENCE

“True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information.”

Sir Winston Churchill

“It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.”

Sherlock Holmes

Information relates to raw, unverified and unevaluated data gathered from numerous source, while, intelligence refers to processed, evaluated and perspective-driven data that is gathered from trusted sources.

INTELLIGENCE > INFORMATION

High Priority Low Priority

Narrow Broad

Signals intelligence (SIGINT)

Imagery intelligence (IMINT)

Measurement and signature intelligence (MASINT)

Human intelligence (HUMINT)

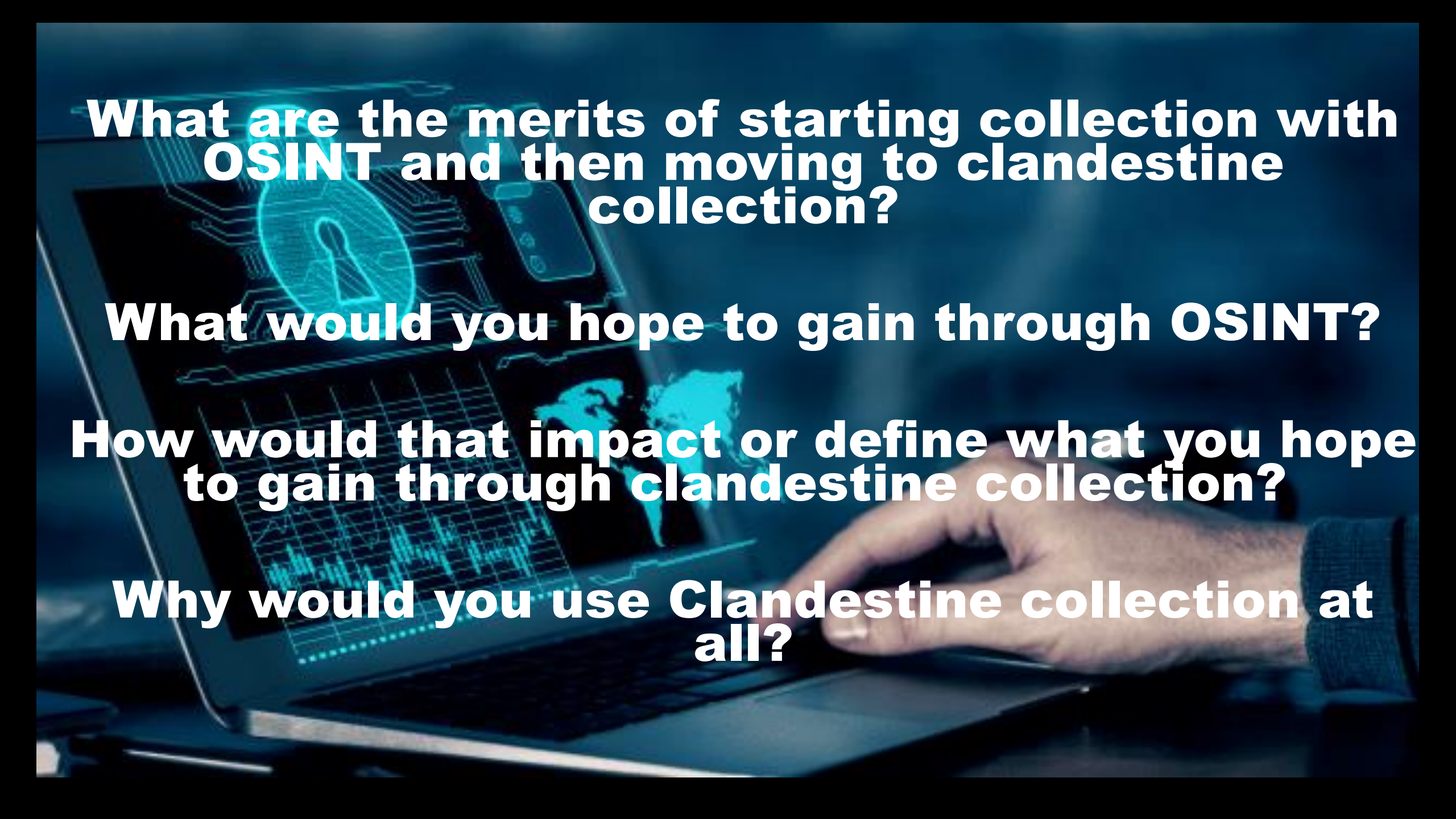
Open-Source intelligence (OSINT)

Geospatial intelligence (GEOINT)

=> Threat Intelligence (TI)

A person's hand is shown typing on a laptop keyboard. The laptop screen displays a world map and a line graph. Overlaid on the screen are digital elements: a large padlock icon, a folder icon, and circuit-like patterns. The entire image has a blue, high-tech aesthetic.

Why do countries collect intelligence?
Should a democracy use Intelligence services?

A person's hand is shown typing on a laptop keyboard. The laptop screen displays a world map and a line graph. Overlaid on the screen are digital graphics, including a glowing blue padlock icon and circuit-like patterns. The background is a dark, blurred image of the laptop and the person's hand.

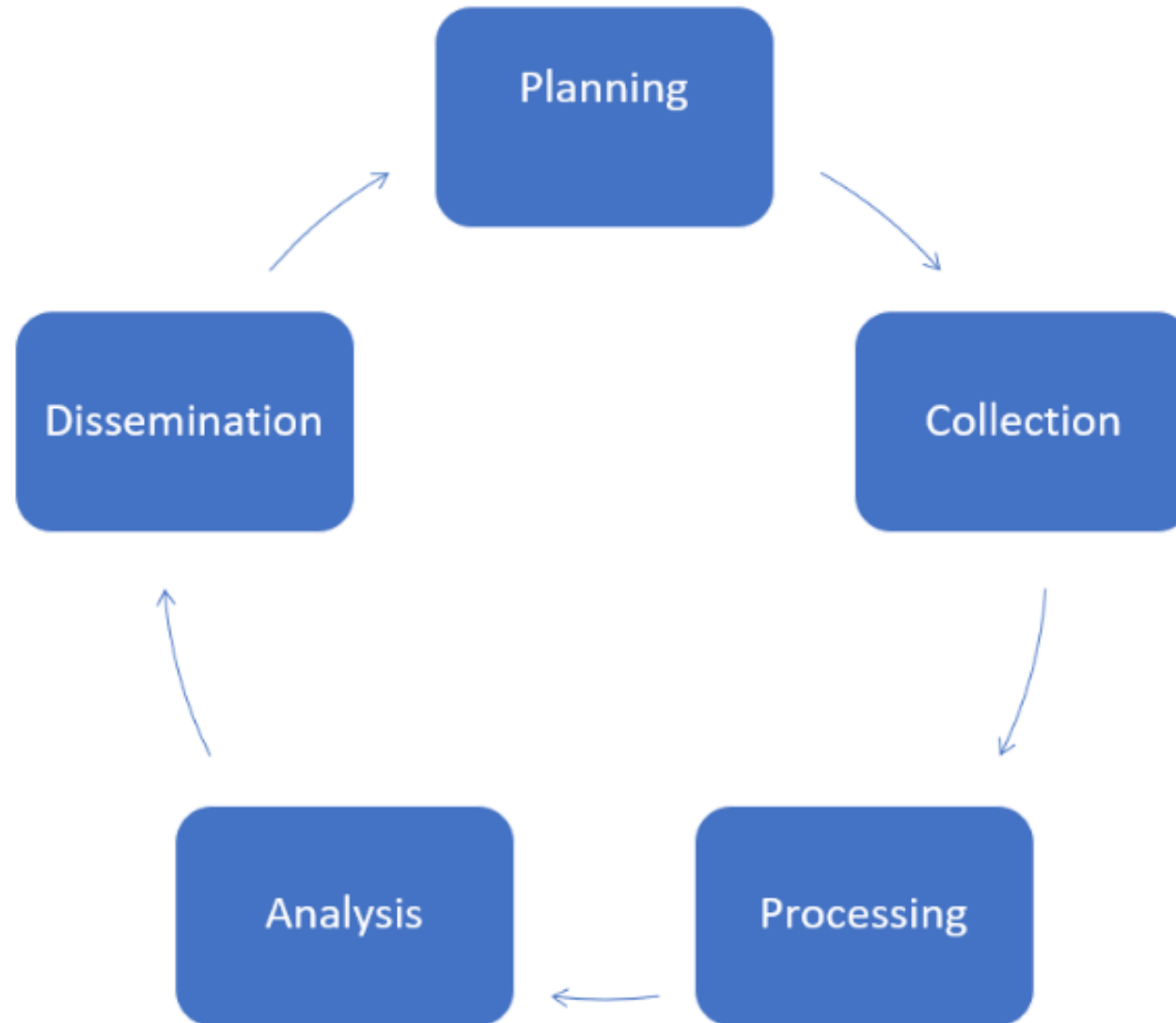
What are the merits of starting collection with OSINT and then moving to clandestine collection?

What would you hope to gain through OSINT?

How would that impact or define what you hope to gain through clandestine collection?

Why would you use Clandestine collection at all?

Cyber Threat Intelligence Life Cycle



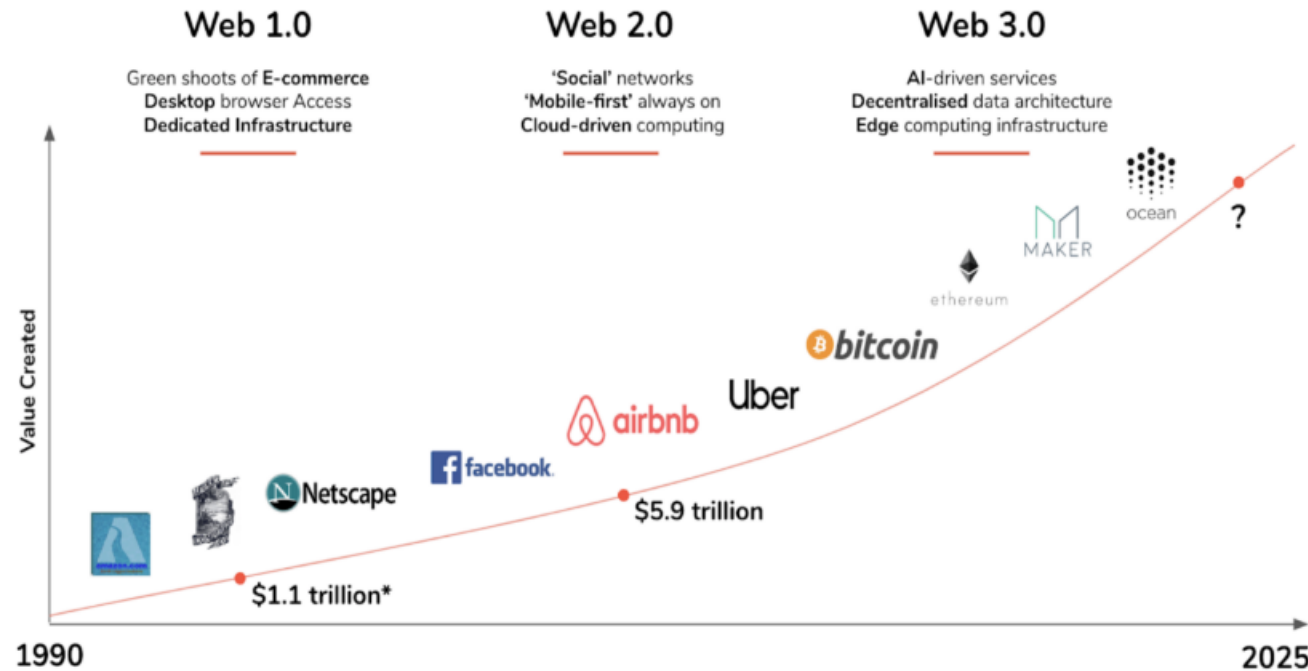
BIG DATA + INTELLIGENCE

Processing Social Media = Conditioning

- a. separates unstructured [floppy] data from structured data;
- b. “collates” the latter, gathering like with like;
- c. facilitates arranging the data in different views/orders;
- d. “assesses” the data for anomalies [bots!], patterns, trends [often for databasing] and for baselining, all by software

Remember: machines “assess”; analysts analyze as in explain in the full historical/political context

The Evolution of the Web



* Internet companies market cap as of 2000

Source: Fabric Ventures

“Web 3.0 is the next generation of Internet technology that heavily relies on the use of machine learning and artificial intelligence (AI). It aims to create more open, connected, and intelligent websites and web applications, which focus on using a machine-based understanding of data.”

A person's hand is shown typing on a laptop keyboard. The laptop screen displays a world map and a line graph. Overlaid on the screen are digital elements: a glowing blue padlock icon, a circuit board pattern, and a glowing blue world map. The background is dark and blue, with a blurred laptop and keyboard.

What are the impacts of social media on OSINT?

Social Media vs. traditional media?

What are the challenges with social media?

Should a democracy use Intelligence services?

Threat intelligence is evidence-based knowledge about an existing or emerging cyber risk. It includes knowledge about mechanism, indicators of compromise (IoCs), impact, implications and actionable advice about the risk, collected through extensive analysis--giving cybersecurity teams enough information about how hackers might attack an organization.

The background image shows a person's hand typing on a laptop keyboard. Overlaid on the laptop screen and the background are several digital, glowing blue elements: a large padlock icon, a smartphone, a world map, and a line graph. The overall color scheme is dark blue with glowing cyan highlights.

How can be prepare to be better OSINT researchers?

Prepare a Structured Source List

**Builds Area Knowledge, Source Expertise, and
buys time forward for Collection and Analysis**

Activity

<https://bit.ly/3TX5QS9>

BYU World Factbook

Countries

Afghanistan	Åland Islands	Albania	Algeria	American Samoa	Andorra	Angola	Anguilla	Antarctica	Antigua and Barbuda	Argentina	Armenia	Aruba	Australia	Austria
Azerbaijan	Bahamas	Bahrain	Bangladesh	Barbados	Belarus	Belgium	Belize	Benin	Bermuda	Bhutan	Bolivia	Bosnia and Herzegovina	Botswana	Bouvet Island
Brazil	British Indian Ocean Territory	Brunei Darussalam	Bulgaria	Burkina Faso	Burundi	Cambodia	Cameroon	Canada	Cape Verde	Cayman Islands	Central African Republic	Chad	Chile	China
Christmas Island	Cocos (Keeling) Islands	Colombia	Comoros	Congo	The Democratic Republic of the Congo	Cook Islands	Costa Rica	Cote D'Ivoire	Croatia	Cuba	Cyprus	Czechia		
Denmark	Djibouti	Dominica	Dominican Republic	Ecuador	Egypt	El Salvador	Equatorial Guinea	Eritrea	Estonia	Ethiopia	Falkland Islands (Malvinas)	Faroe Islands	Fiji	Finland
France	French Guiana	French Polynesia	French Southern Territories	Gabon	Gambia	Georgia	Germany	Ghana	Gibraltar	Greece	Greenland	Grenada	Guadeloupe	Guam
Guatemala	Guernsey	Guinea	Guinea-Bissau	Guyana	Haiti	Heard Island and McDonald Islands	Vatican City State	Honduras	Hong Kong	Hungary	Iceland	India	Indonesia	Iran
Iraq	Ireland	Isle of Man	Israel	Italy	Jamaica	Japan	Jersey	Jordan	Kazakhstan	Kenya	Kiribati	North Korea	South Korea	Kuwait
Kyrgyzstan	Laos	Latvia	Lebanon	Lesotho	Liberia	Libyan Arab Jamahiriya	Liechtenstein	Lithuania	Luxembourg	Macao	Macedonia	Madagascar	Malawi	Malaysia
Maldives	Mali	Malta	Marshall Islands	Martinique	Mauritania	Mauritius	Mayotte	Mexico	Micronesia	Moldova, Republic of	Monaco	Mongolia	Montserrat	Morocco
Mozambique	Myanmar	Namibia	Nauru	Nepal	Netherlands	Netherlands Antilles	New Caledonia	New Zealand	Nicaragua	Niger	Nigeria	Niue	Norfolk Island	Northern Mariana Islands
Norway	Oman	Pakistan	Palau	Palestinian Territory, Occupied	Panama	Papua New Guinea	Paraguay	Peru	Philippines	Pitcairn	Poland	Portugal	Puerto Rico	Qatar
Reunion	Romania	Russian Federation	Rwanda	Saint Helena	Saint Kitts and Nevis	Saint Lucia	Saint Pierre and Miquelon	Saint Vincent and the Grenadines	Samoa	San Marino	Sao Tome and Principe	Saudi Arabia	Senegal	
Serbia and Montenegro	Seychelles	Sierra Leone	Singapore	Slovakia	Slovenia	Solomon Islands	Somalia	South Africa	South Georgia and the South Sandwich Islands	Spain	Sri Lanka	Sudan		
Suriname	Svalbard and Jan Mayen	Swaziland	Sweden	Switzerland	Syrian Arab Republic	Taiwan	Tajikistan	Tanzania	Thailand	Timor-Leste	Togo	Tokelau	Tonga	
Trinidad and Tobago	Tunisia	Turkey	Turkmenistan	Turks and Caicos Islands	Tuvalu	Uganda	Ukraine	United Arab Emirates	United Kingdom	United States	United States Minor Outlying Islands			
Uruguay	Uzbekistan	Vanuatu	Venezuela	Vietnam	British Virgin Islands	U.S. Virgin Islands	Wallis and Futuna	Western Sahara	Yemen	Zambia	Zimbabwe			

+

Switzerland

+

Advanced Persistent Threats

>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in

Advanced Persistent Threats

Indicators of Compromise Categories:

- Example for Vietnam -
 - Spearphishing [Ocean Buffalo]
- Iran:
 - Spearphishing middle-aged male engineers with explicit content [Charming Kitten]

Media Landscape:

- What government agencies or subgroups of the military control certain media outlets?
- How restricted are media channels? (Think China)

Social Media Landscape:

- What social media outlets are usable/restricted in the country?
- What is percentage of users?
- Unique/proprietary Social media platforms?
 - Political skew of these platforms?

ISP Registrar:

- Example for Japan:
 - Spinnet – Information...
 - ASAHI Net – Information...
 - au Hikari – Information...
 - Softbank – Information...

Security/Privacy Regulation:

- What are the privacy policies and laws (data, personal info, etc.)?

Transnational Issues:

- International disputes
- Refugee Issues
- Drug Issues
- Terrorism

Political Opposition:

- Recognized parties in opposition of nation-state
- Political ideology clashes

Useful Resources

- FreedomHouse.org
- RSF.org
- InternetWorldStats.com
- CIA World Factbook - <https://www.cia.gov/the-world-factbook/>