Chinese Censorship: The Dark Web Tipping Point for Indo-Pacific Operations

CACI

EVER VIGILANT

This material consists of CACI International Inc general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-10. (PRR ID 493) (3/18/2022)

Contents

Executive Summary

In the emerging cyber domain where social media and the proliferation of modern technology provide users the unprecedented ability to create and transmit large amounts of data, Joint-All Domain Command and Control (JADC2) elements leverage Open-Source Intelligence (OSINT) platforms to understand the myriad of actors and communications dynamically shaping conflicts globally. Yet, even after OSINT is propelled into a position of indispensability, the picture remains incomplete. Autocratic censorship of open web data forces users deep below the surface web and into the virtually ungoverned spaces of the internet, known as the Deep and Dark Web, where our opponents dominate, threat actors operate, and critical information proliferates. Without specialized technology, tradecraft, and analyst expertise to access these denied areas beneath the surface web, JADC2 will continuously struggle to achieve decision dominance in the cyber domain. Within this report, Bluestone Analytics reviews findings from the Dark Web, addresses the relevancy of Dark Web research and analysis, and provides key recommendations for agencies and organizations.

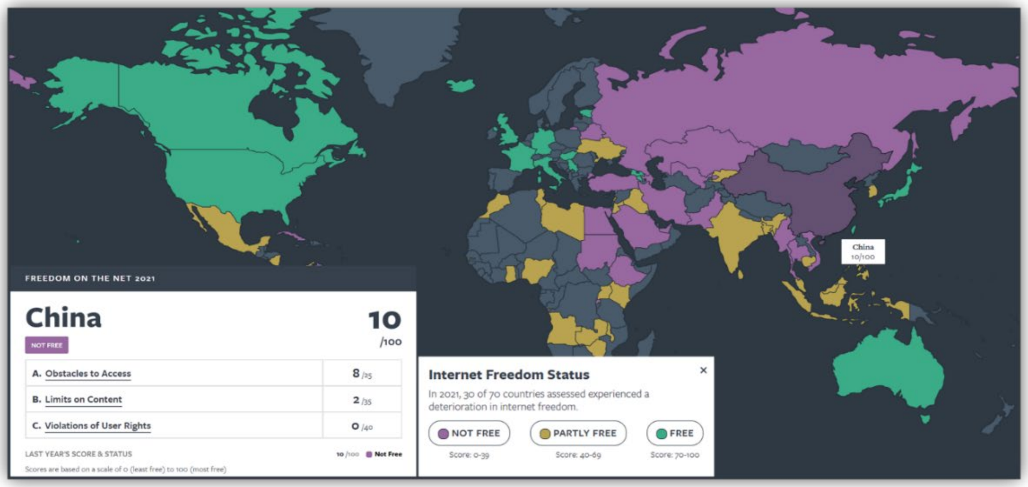
About Bluestone Analytics

Bluestone Analytics, a CACI Company, is the established leader in Dark Web exploitation and analysis. Our mission-focused technology suite, DarkBlue Intelligence, is coupled with analyst-led training and tailored services that empower clients to operate within hidden portions of the Information Environment effectively. Bluestone Analytics provides National Security, Intelligence, and Law Enforcement communities with safe, persistent, holistic access to identify, target, and track Dark Web threat actors globally. To learn more, visit www.bluestoneanalytics.com

This material consists of CACI International Inc general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-10. (PRR ID 493) (3/18/2022)

Censorship Challenges in the Indo-Pacific Theater

The differences in how digital communications and social media are governed among countries in each area of responsibility (AOR) create warfighting asymmetries. According to a 2021 Freedom of the Net (FOTN) report[1], countries assessed as "not free" tend to be those with autocratic forms of government, such as China and Russia. Governments in these countries control the narrative through censorship, blocking, and filtering communications and content. For example, the notorious "Great Firewall of China" drives citizens to find alternative connections and operate deep below the Surface Web in ungoverned spaces of the internet that are hard to reach or impossible to block[2]. The U.S. National Security Community largely misses what's "below the surface" – the Deep and Dark Web.



FREEDOM ON THE NET 2021

China

NOT FREE

10 /100

A. Obstacles to Access	8 /25
B. Limits on Content	2 /35
C. Violations of User Rights	0 /40

LAST YEAR'S SCORE & STATUS 10 /100 ● Not Free

Scores are based on a scale of 0 (least free) to 100 (most free)

Internet Freedom Status

In 2021, 30 of 70 countries assessed experienced a deterioration in internet freedom.

● NOT FREE Score: 0-39

● PARTLY FREE Score: 40-69

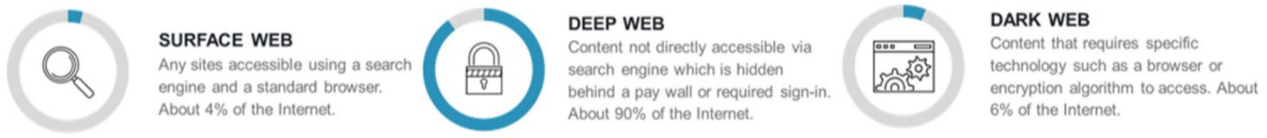
● FREE Score: 70-100

Figure 1. 2021 Freedom of the Internet Report

Below the Surface – The Deep Web and Dark Web

The Surface Web, or Open Web, comprises only four percent of the content on the internet and stands as the most familiar portion of the internet. Crawled and indexed by search engines like Google, its Domain Name System (DNS) maps domain names to the numerical I.P. addresses to locate services and devices using underlying network protocols.

The Deep Web and Dark Web have a primary, common characteristic: they are difficult to reach. The Deep Web comprises roughly 90 percent of the content on the internet that is not directly accessible via a search engine. This portion of the internet is gated behind several variances of login or paywalls. The Dark Web is a much smaller subset, comprising only six percent of the content on the internet. The Dark Web is distinguished from the Open Web and the Deep Web in that it requires specialized encryption or browsers to gain access. It is a dynamic, anonymous environment, originally designed to provide a secure communication channel to individuals in high-risk countries, consisting of a collection of dark nets such as Tor, I2P, and Zeronet.



SURFACE WEB
Any sites accessible using a search engine and a standard browser. About 4% of the Internet.

DEEP WEB
Content not directly accessible via search engine which is hidden behind a pay wall or required sign-in. About 90% of the Internet.

DARK WEB
Content that requires specific technology such as a browser or encryption algorithm to access. About 6% of the Internet.

Figure 2. Defining the Surface, Deep, and Dark Web

[1] Freedom House. (2022). Freedom on the Net. Retrieved from https://freedomhouse.org/report/freedom-net

[2] Zhou, Q. (2020, December 28). Building the (fire) wall: Internet censorship in the United States and China. Retrieved from Harvard International Review: https://hir.harvard.edu/building-the-fire-wall/

Dark Web Relevancy

While initially funded by the U.S. Government to allow users under autocratic systems to bypass censorship and organize online, dark nets deliver anonymity while surfing the Dark Web or publishing information. This anonymity facilitates the communication of sensitive data for legitimate purposes. However, this anonymity also provides the ideal environment for nefarious actors to transfer information, goods, and services with potentially illegal or hostile intentions. As the virtual domain continues to expand, the Dark Web becomes the emerging space to conduct virtual operations and leverage near real-time information of intelligence value, including Great Power Competition (GPC) activities, indication and warnings (I&W), propaganda, influence, and counterintelligence activities.

Chinese Users Across the Dark Web

Chinese users can securely and anonymously access the Dark Web through a series of dark net browsers, such as Tor and ZeroNet. These dark nets provide users with unique experiences and security elements to conduct business and communication to bypass government censorship. Chinese populations, for example, exhibit different behavior patterns depending on the dark net they are using.

- **Tor[3]:** The Tor network remains the most popular dark net for users due to its accessibility and security. Tor's ease of use and diverse content attracts millions of international users. Chinese users have utilized the Tor network for markets selling Chinese-related content and language-specific forums and chatrooms.
- **ZeroNet[4]**: ZeroNet caters to diverse international populations seeking content or facilitating conversations deemed illegal or heavily moderated in their country. Chinese users who gravitate to ZeroNet are more inclined to publish anti-Chinese Communist Party (CCP) messages or promote content that would be censored on other platforms. Through further monitoring and analysis of Dark Web data, it was discovered that Chinese users accessing ZeroNet sites engage more openly in criticizing the Chinese government and converse about developing social situations occurring inside China.

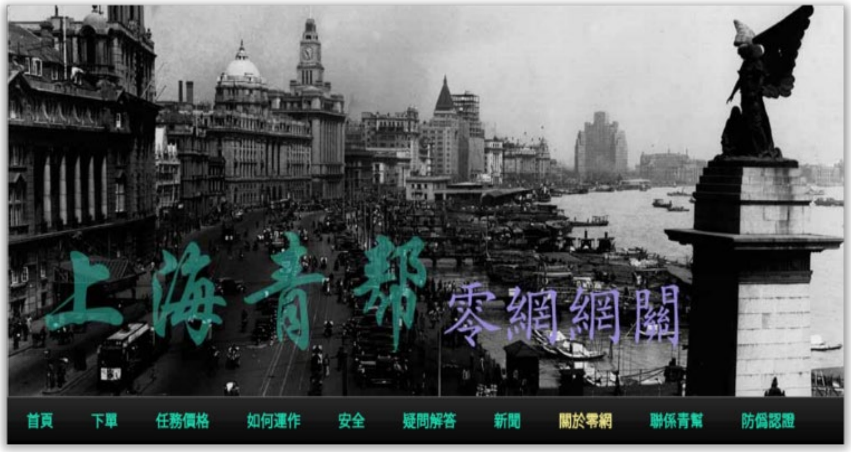


Figure 3. Anti-CCP / Humanitarian Rights Website on ZeroNet

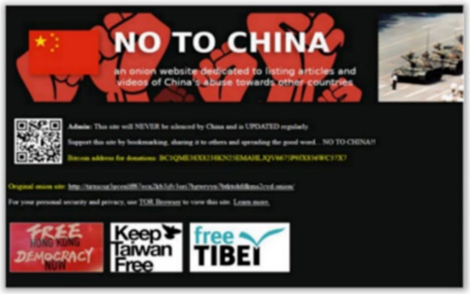
[3] Tor, aka The Onion Router, operates on an encrypted network of publicly available Tor nodes that are hosted on a decentralized volunteer network, which are used to anonymize user traffic. The Tor network also allows users to have dual-access points to either Dark Web or Open Web content.

[4] ZeroNet is a dark net that operates on a decentralized, censorship-resistant network. The infrastructure of ZeroNet utilizes cryptography and BitTorrent technology. ZeroNet is not anonymous by default and users that are aware of this vulnerability will use ZeroNet in conjunction with the Tor browser.

This material consists of CACI International Inc general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-10. (PRR ID 493) (3/18/2022)

Combatting Censorship | NO TO CHINA

The Dark Web was initially designed to be a space for free speech by democracy advocates within restricted nations to share information regarding local conditions and human rights issues that would be censored on the Open Web. Despite the CCP's attempts at censoring Dark Web content for those accessing Tor Nodes from China, Dark Web users have used specific tactics, techniques, and procedures (TTPs) to bypass CCP restrictions and publish anti-CCP information. These TTPs include posting Chinese censored terms which boot any users in China from a forum, hosting blogs on different dark nets to avoid detection, and publishing information on various Tor sites to educate users on the actions of the CCP.


NO TO CHINA
an onion website dedicated to listing articles and videos of China's abuse towards other countries

Admin: This site will NEVER be silenced by China and is UPDATED regularly

Support this site by bookmarking, sharing it to others and spreading the good word... NO TO CHINA!!

Bitcoin address for donations: [illegible]

Original onion site: [illegible]

For your personal security and privacy, use TOR Browser to view this site. Learn more.

FREE HONG KONG DEMOCRACY NOW
Keep Taiwan Free
free TIBET

Figure 4. NO TO CHINA Published Anti-China Articles and Videos

NO TO CHINA[5] is a Tor site dedicated to publishing articles and videos critical of the Chinese government to provide Chinese Dark Web users access to uncensored news. NO TO CHINA has been operational on Tor since 2014 but ramped up activity in recent years due to the events of Hong Kong and COVID-19. Banners at the top of the site re-direct users to Open Web sites dedicated to Free Hong Kong[6], Keep Taiwan Free[7], and Free Tibet[8].

Conclusion and Recommendations

Published data on the Dark Web is invaluable. For many agencies and organizations, allowing Dark Web information to remain a blind spot is risky at best. Monitoring the Dark Web has the potential to unveil data and intelligence that simply couldn't be found anywhere else. Initial challenges include safely leveraging and engaging within ungoverned virtual environments where our opponents dominate, threat actors operate, and critical information proliferates. Two primary recommendations include:

1. **Conduct risk and vulnerability modeling** of the latest TTPs gaining traction in the cybercriminal underground.
2. **Incorporate open-source monitoring** into mitigation and response strategies to easily comb through and prioritize Dark Web threat activity.

Bluestone Analytics, a CACI Company, has integrated into hundreds of Dark Web communities and places where most cannot infiltrate. Our award-winning DarkBlue Intelligence Suite provides access to over 6B records of data, robust search and filtering capabilities, and leading analytical tools in a single intuitive interface. As a trusted, US-based vendor providing Software-as-a-Service (SaaS) and Data-as-a-Service (DaaS) platforms, we have empowered DoD, Intelligence, National Security, Law Enforcement, and Other Government Agencies (OGA) to understand and operate across the ungoverned virtual environment rapidly.

Our advanced intelligence and machine learning (AI/ML) technologies enhance mission speed in the virtual domain by reducing the cognitive load, effectively enabling the JADC2 vision of decision dominance. We provide approved, commercially acquired technology capable of integrating with current OSINT and classified data platforms, distinguished through four key pillars:

- Collect, curate, and enhance data that is otherwise elusive and difficult to obtain
- Deploy advanced technology to analyze data, operate virtually, and deliver effects
- Provide an expert staff to enable client missions
- Innovate ahead of current client requirements

[5] NO TO CHINA - tirxscsg3pcenlff67ecn2kb3jfv3ori7bgwryyn7btktohfdkms2cyd.onion [Requires Tor Browser]
[6] Free Hong Kong - freehongkong.org [Open Web site]
[7] Keep Taiwan Free - keeptaiwanfree.org [Open Web site]
[8] Free Tibet - freetibet.org [Open Web site]

This material consists of CACI International Inc general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-10. (PRR ID 493) (3/18/2022)