

CYBER INTELLIGENCE: PUT THE POWER OF THE WEB TO WORK FOR YOUR ORGANIZATION

Leveraging actionable intelligence for a proactive approach to due diligence, litigation and research offers a competitive edge

“I did then what I knew how to do. Now that I know better, I do better” (Maya Angelou)

The breadth of information and data stored in the Internet is endless, and new information is constantly generated. But it can be a case of “water, water everywhere and not a drop to drink.” Successfully navigating the Web to find the *right information and intelligence* can be a complex exercise, but the rewards are worth it – winning cases and avoiding crucial mistakes. This is the crux of Cyber Intelligence.

Cyber Intelligence might sound like an intimidating technical term, but it’s actually quite simple to learn and apply in our daily work. It is the art of collecting intelligence from around the Web, getting access to the most critical information we need, and analyzing it quickly and accurately. Cyber Intelligence requires more analytical thinking than technical skills, which is why it’s becoming a trend among analysts, lawyers, bankers and other professionals who see the potential of a proactive Web approach. Cyber Intelligence is the complement to Cyber Security, which focuses on protecting our information and networks.

Some of the most common Cyber Intelligence skills include:

- Advanced search techniques and methods to uncover hidden data and recover deleted data from around the Web
- Deep due diligence and building a profile of a company or a person
- Creating information alerts and automatic search notifications
- Analyzing metadata and digital evidence
- Accessing the “Dark Web” and financial crime platforms

Cybint has worked for the past 13 years with financial institutions, law firms and other companies, and observed multiple instances where Cyber Intelligence resulted in avoiding critical mistakes and creating a strong advantage over rivals. We’d like to share three ways Cyber Intelligence can provide the competitive edge:

Cyber Intelligence in due diligence (M&A, investments, senior level hire, etc.)

Representations and warranties are no longer sufficient to close a deal or underwrite potential losses. Using Cyber Intelligence in due diligence adds significant value to every merger, acquisition, investment or other transaction. With Cyber Intelligence skills, we can:

- Identify suspicious changes the opposing party made prior to the due diligence process by *recovering online deleted information*
- Track claims against the target company through *access to hidden information*
- Identify theft and leaks of Intellectual Property through *Deep Web and Dark Web analysis*
- Analyze reputation issues through *scanning social networks*, and identify the public sentiment toward the company, and identify dissatisfaction of employees through *accessing reputation tools*
- Identify whether the target company is growing or declining through *online traffic analysis*
- Verify or disprove claims of the other side through *advanced search and tools*
- Better KYC - Collecting information and identify “red flags” among clients and partners, through *various databases, social networks, deleted information, leaked information, online reviews, etc.*

Cyber Intelligence in negotiations, disputes and litigation

Identifying relevant information about the case and the opposite side is critical to gaining an advantage in negotiations, disputes and in court. Cyber Intelligence critically affects the strategy and advice attorneys and financial professionals can give their clients. With Cyber Intelligence skills, we can:

- Strengthen the evidential foundation of our case through *finding critical information* that the opposing side deleted from the Web or hid from search engines
- Determine if a photo was photo-shopped or a document was edited through *analyzing metadata of images, documents and videos* – finding who created them and when, what kind of software\camera\tool was used to create them
- Identify contradictions in testimonies and affidavits through *identifying past statements, locations or activities of the rival side*
- Have all the new critical information about the case sent directly to our email through *developing a set of information alerts through websites, search engines, RSS files and more*
- Improve success rates in cases through *producing actionable intelligence*

Cyber Intelligence in financial crime investigations

Cyber Intelligence gives us a deeper understanding of the deep and Dark Web, with an intimate look into the online ecosystem of financial crimes and cyber criminals. This knowledge and these skills are critical to analysts, investigators, financial crime specialists, prosecutors and lawyers who deal with complex financial cases. With Cyber Intelligence skills, we can:

- *Get access to the Dark Web* using TOR, P2P, Proxies and additional tools
- *Track money transfers of cybercrimes* into the Dark Web
- *Identify financial criminals by matching identities* in the Dark Web to “real people”
- *Prevent digital frauds and cybercrimes before they happen*, using threat intelligence methods
- *Identify and analyze criminal trade platforms* using Dark Web search engines

These three examples represent just a few of the many ways we can utilize Cyber Intelligence in business activities. There are numerous other uses in legal, financial and business environments. This proactive approach to managing due diligence, litigation and research, shouldn't be just the work of investigators; it's well within our capabilities as attorneys, financial professionals and analysts to integrate Cyber Intelligence knowledge, skills and tools in our daily work. It will allow us to **know better and do better for ourselves and our clients.**