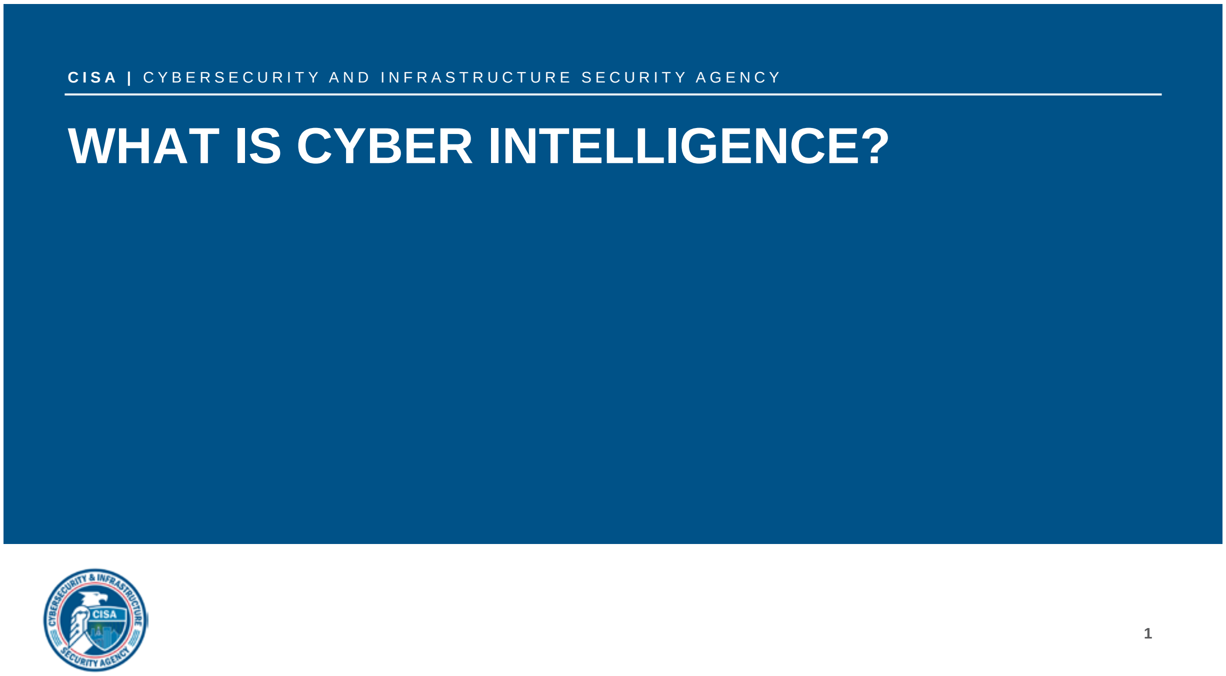
What is Cyber Intelligence?

Table of Contents

What is cyber intelligence?



CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

WHAT IS CYBER INTELLIGENCE?

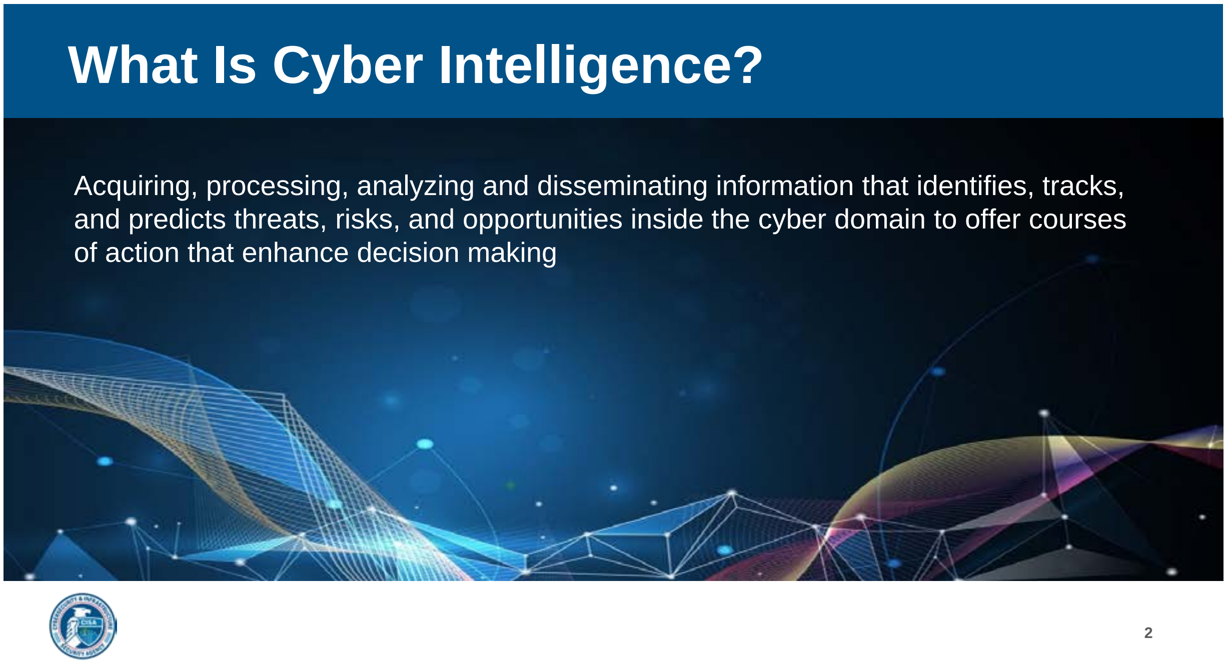
1

**001 Instructor: So, let's talk about cyber intelligence. What is it? We asked 32 organizations representing 10 of 16 DHS critical infrastructure sectors in our 2019 study to define key words such as cybersecurity, cyber intelligence, cyber threat intelligence, tactical, operational and strategic intelligence. We got a ton of different answers. We found, and perhaps not surprisingly, that words mean different things to different people, shaped by our own unique experiences and backgrounds.

While getting different perspectives in encouraged, the lack of a common cyber lexicon makes it challenging for teams and organizations across sectors that we interviewed to arrive at a common ground for solving complex cyber problems. The reason for this is because how we understand words leads to actions on those understandings. We operationalize our actions.

So we thought a shared lexicon about keywords will increase collaboration, create trust and common actions. In our report, we provide clarity on these terms, cyber intelligence, cybersecurity, cyber threat intelligence and others, and based on the definitions that we received, we define cyber intelligence as the following.

What Is Cyber Intelligence?



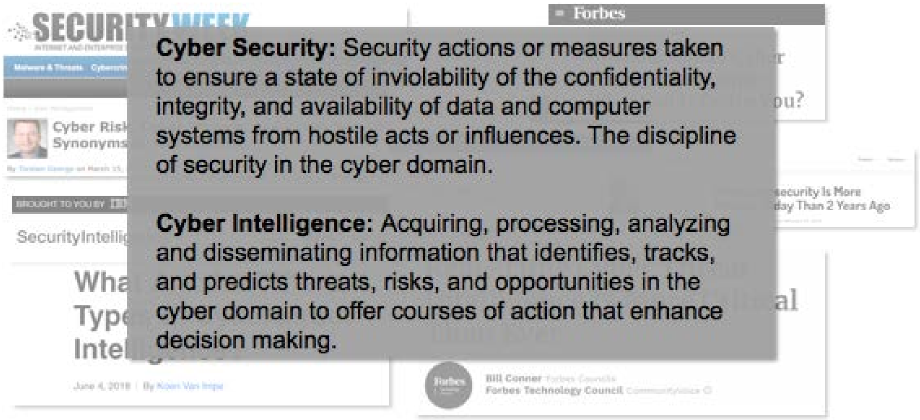
What Is Cyber Intelligence?

Acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making

**002 Cyber intelligence is acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making. But wait a second. You might be asking, "What is cybersecurity? What is cyber threat intelligence, and how are they different?"

.Need for a Common Lexicon

Need for a Common Lexicon



Cyber Security: Security actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences. The discipline of security in the cyber domain.

Cyber Intelligence: Acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.

**003 So an organization may protect the confidentiality, integrity and availability of data and computer systems. Such practices, based on our research, falls into the realm of cybersecurity. Cybersecurity's literally the discipline of security inside the cyber domain. So what does that really mean?

Based on definitions that organizations gave us, fused with some terminology we pulled, excuse me, from DHS's own publicly available information, we define cybersecurity in our report as security actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences.

You know, we also heard the term cyber hygiene during our interviews, and that tends to be referred to both cybersecurity and as actions to improve cybersecurity. Cyber hygiene actions could be vulnerability scanning, patching systems, ensuring compliance, protecting network infrastructure or inventorying hardware or software assets, configuring firewalls and other products. Cyber intelligence is not that. It is not cybersecurity and it is not cyber hygiene.

Indeed, now, one might ask, "Does your organization know which threat actors have the potential to target your organization now and in the future? Which of your patent-pending technologies are at risk? How might threat actors attack your organization? Why do they want to attack your organization, and how would certain attacks impact your organization's mission and vital interests from holistic perspective?"

Even does your organization track malware campaigns or perform supply chain threat analysis? Or is it doing assessments on the impact and opportunity of emerging technologies on business and industry?

These are the types of questions that cyber intelligence can help answer and that high-performing cyber intelligence teams we met are actually working on. So cyber intelligence literally is the discipline of intelligence in the cyber domain, and more specifically, based on our interviews, we define it again as acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action to enhance decision making.

I want to make another comment about terms. A number of organizations we met express confusion, and some even slight irritation trying to decipher the difference between cyber threat intelligence and cyber intelligence. Specifically are these terms the same thing? These organizations commented that introducing the word threat into the cyber intelligence vernacular was not too beneficial, because cyber threat intelligence conveys something distinct from cyber intelligence, and for those organizations, intelligence is intelligence no matter the concern or issue being analyzed.

In other words, intelligence analysis can be performed to produce cyber intelligence products about threats, risks and opportunities, technologies, geopolitics, involving people, groups, companies and nation-states, and while intelligence analysis on threats was absolutely the major focus of organizations we interviewed, by all means though it was not the only focus of cyber intelligence teams, and because of this, our report offers that cyber intelligence should be understood as an umbrella term.

A way to conceptualize this is that under the umbrella hood of cyber intelligence includes cyber threat intelligence, but cyber threat intelligence does not represent all of cyber intelligence, and when I talk about opportunities, it can mean everything from getting insight into mergers and acquisitions, developments in your own industry, technology development such as 5G or business opportunities with more people being connected to the internet in the coming years. It could mean, especially in the intelligence in defense or military circles, targeting, recruitment and other operations.

.Notices

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM20-0262