Cyber Intelligence - Skills, Traits, Competencies

Table of Contents

Cyber Intelligence – Skills, Traits, Competencies

Cyber Intelligence – Skills, Traits, Competencies

9

**009 From our first research with the Cyber Intelligence Tradecraft project from 2013, we met with almost 30 companies, and they gave us some insight into the skills, traits, and competencies that are needed to be a successful cyber intelligence analyst.

Analysts Being Hired 2013

Retired Military Communications Officer

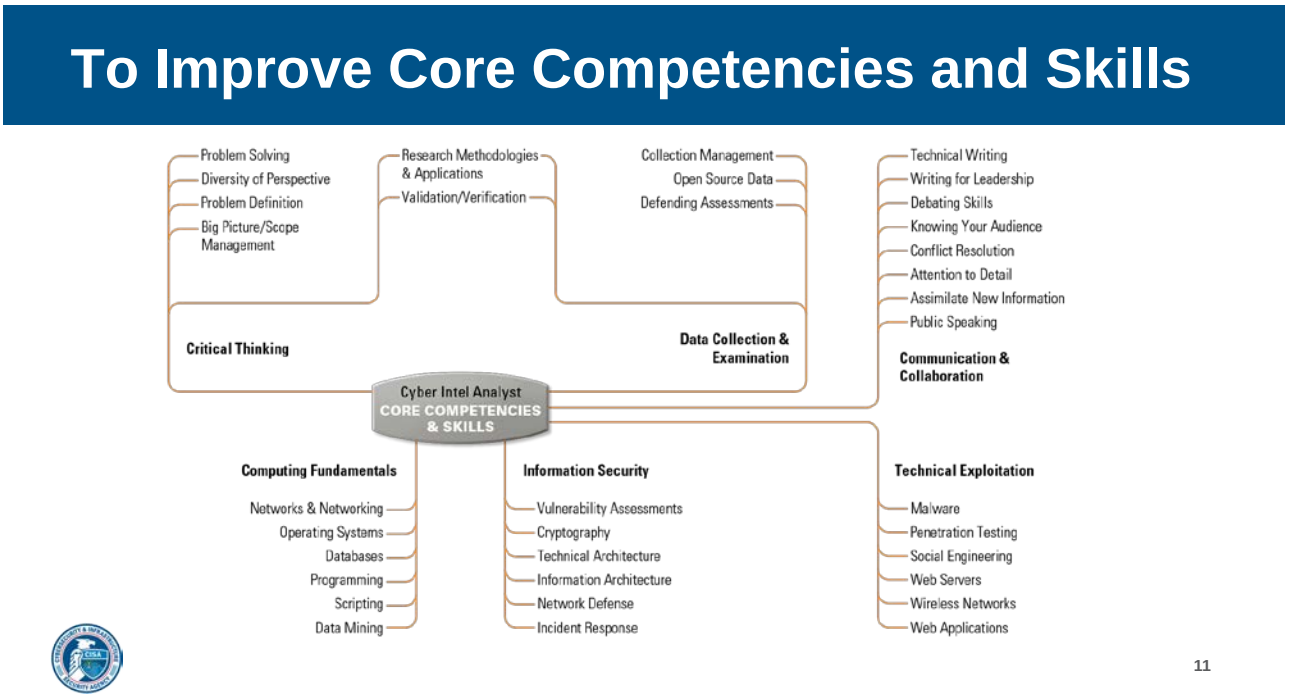
Information Technology Professional

Liberal Arts Graduate

10

**010 Back then, in 2013, the field was kind of split across intel analysts, information technology professionals, and liberal arts graduates. Companies were hiring intel analysts and training them on tech, or hiring IT folks and training them on how to do intel. Or some would just prefer a Liberal Arts degree and find those types of individuals who are capable of thinking critically and communicating effectively. Finding one person with all these traits was and remains today not easy, so we put together back then a whitepaper as part of the report that digs deeper into the skills, traits, and core competencies from 2013. Many organizations still refer to it.

To Improve Core Competencies and Skills



**011 It looks something like this. Here are some additional core competencies and skills that were important for a cyber intelligence analyst in 2013. They're kind of--they're might be a little bit blurry, so I'll read a few for you now. Critical thinking. That's where you have problem-solving skills, diversity of perspective, being able to see the forest from the trees, or data collection and examination.

In other words, how do you collect data? What is important to collect and how do you know? When do you know the infor--what do you know when the information comes in and where does it come from?

Communication and collaboration. Are you able to write technically and

communicate those technical findings to a non-technical person?

Computing fundamentals. So no one person may have all these computing fundamentals. In fact, most don't, and that is fine. These are just listed in a way as competencies and skills that we found, such as programming and scripting and understanding operating systems, networks and subnets.

Information security, incident response, cryptography or information architecture and technical exploitation, such as pen testing skills, social engineering, building and establishing web application tools.

Cyber Intelligence Skills, Traits, Competencies Today

**012 What we found today, and document in our most recent research, is that there's still a gap

between technical and analytical expertise. Indeed, we state that a gap remains and is widening between individuals experienced in intelligence analysis and operations and those experienced in information security, computing fundamentals, and artificial intelligence.

Some organizations today have only technical people on their team with zero or--to little understanding or background and training in intelligence analysis. Other organizations that employ individuals experienced in intelligence analysis and information security encounter stark cross-team communication challenges.

This list of skills, traits, and core competencies is from our 2019 study. We literally asked organizations what they look for in threat analysts or the more technical analysts or strategic analysts, and here is a list. The threat analysts typically have computing fundamentals or cybersecurity, technical exploitation, intrusion analysis skills, incident response analysis skills and experience, vulnerability analysis.

For strategic analysts the list is a little bit shorter, but they have a general understanding of technical concepts that threat analysts or more technical analysts have. Strategic analysts usually have critical thinking skills, problem-solving skills. They understand geopolitics. They can Communicate effectively and have intelligence analysis skills.

All of these skills and much more, such as data science skills, machine learning engineers, are needed

Bad Guys – Good Guys

**014 The reality is that there's more threats, more types of threats, and the sophistication of these threats and threat actors has increased. We are seeing hacking knowledge and corresponding tools being democratized. We continue to experience an imbalance when it comes to the good guys verse the bad guys, and the scholar Jason Healy talks about this asymmetry. You know, he tells us that a dollar an hour of cyber offense, attacking, those bad guys, outspends a dollar a hour of cyber defense, us, the good guys.

So from a bad guy's perspective it costs about $60 for renting

infrastructure for DDoS, for example, or $50 for a social media account takeover, even $14 for passport scans. Cybercrime, on the flip side, will cost the world 6 trillion dollars annually by 2021, according to Cyber Ventures. The average cost of a data breach in 2019 was 3.92 million, according to IBM, and according to the website fortunately, the cost of cyberattacks in the banking industry reached 18.3 million annually per company.

It is estimated that the spending of cybersecurity training will reach 10 billion dollars by 2027. So for us to get this right, we have to reverse the trend. We need to make the attackers spend more time, more money, more effort and resources. But how do we reverse this trend?

One way is with cyber intelligence. Specifically, best practices that involved--

Reverse the Asymmetric Trend

**015 --truly and deeply understanding your organization's environment, which enables you to collect the right data, analyze the data, and then make recommendations to your decisionmakers so that they can take courses of action to enhance your organization's overall risk posture. It's also important to stay current and up-to-date on technological advancements to include AI and machine learning.

Limit Tunnel Vision or Mirror Imaging

- By understanding all the causes and effects of potential threats

16

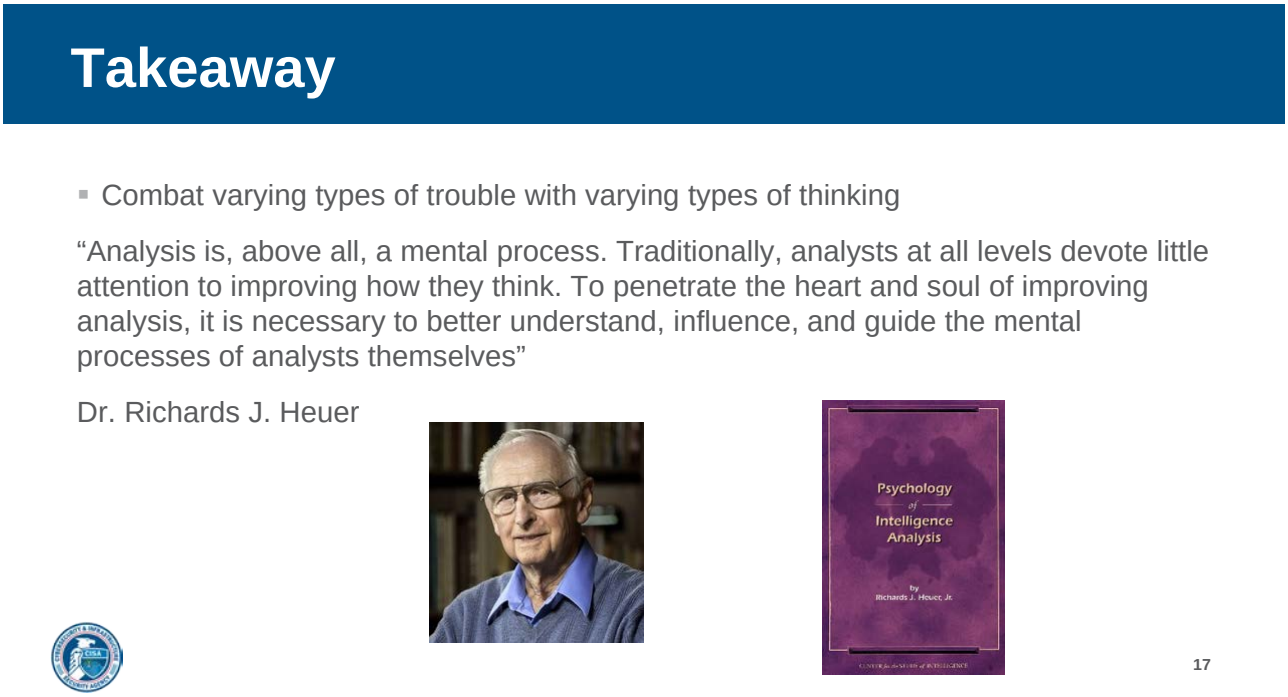
**016 Additionally, I would tell you that reversing the trend in many ways boils down to improving how we think about intelligence and how we do intelligence. Because if we get this wrong, if we are unable to think holistically, if we're unable to challenge traditional thoughts and not look for just that perfect tool or technology to solve our problems, then we're going to get this wrong no matter how much or how little we spend.

For example, if you have tunnel vision or mirror imaging, saying, "Well, you know, we think the threat actor will do xyz, because if we were in their shoes we would also do xy and z," then what you're ending up doing is providing intelligence to a decisionmaker who might end up

using that information and then make a serious error in judgment.

We need to limit tunnel vision and think holistically. A pioneer in intelligence, in the intelligence world for thinking holistically, was Dr. Richard Heuer.

Takeaway



**017 What Dr. Heuer said, or studied, was looking at intelligence as a profession and how to better train analysts how to think critically. In other words, why do we think the way we think? What do analysts think about? What are the challenges that prohibit or impede the mental process, and are there ways to train ourselves to think differently about different things and about the same things? To look at all perspectives, to know when to say

that you know something, believe in something, or that you do not know something is extremely important. Important decisions will be made based on what and how you communicate.

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.

DM20-0262