VB2020
localhost

30 September - 2 October, 2020 / vblocalhost.com

2030: BACKCASTING THE RISE AND FALL OF CYBER THREAT INTELLIGENCE

Jamie Collier
FireEye, UK

jamie.collier@mandiant.com

ABSTRACT

The year is 2030. After encouraging growth in the early 2020s, the cyber threat intelligence (CTI) industry has almost entirely collapsed. Many of the leading CTI vendors have gone bankrupt. Most professionals working in the industry have transitioned to other cybersecurity functions.

This talk will explore what went wrong. The presentation will use backcasting as an analytical technique to create this imagined future and highlight hypothetical hazards in the CTI industry. These include CTI functions ostracizing themselves from security and leadership teams, failing to respond to developments in the market, and distorting coverage of the threat landscape.

The talk is neither a prediction nor intended as an industry hit job. Instead, it will provide an opportunity to reflect on where we are as an industry, anticipate potential pitfalls, and consider how CTI practices can improve. This paper therefore seeks to make a positive case for how the industry can continue to thrive.

INTRODUCTION

Among the IPOs, consistent growth and growing public profile, it is easy to forget just how young the CTI industry is. As with any nascent market, a reflective culture is critical. The CTI industry excels at covering the threat landscape, ranging from North Korean heists to mobile malware developments. Yet, questions on the future direction of the industry are comparatively underexplored.

This paper seeks to redress this imbalance through science fiction (albeit a tame version that excludes any mention of cyborgs or vivid cyberpunk references). Instead, through a backcasting exercise, this paper will imagine the future collapse of the CTI industry. While a large degree of creative freedom has been allowed, it is hoped that this will help probe questions around the current status of the CTI industry and the potential pitfalls that could lie ahead.

The CTI industry sits in an exciting space. The majority of those working in CTI see their job as a vocation – a mission that is inherently interesting and filled with purpose. CTI improves cybersecurity outcomes for business, governments and society. Providing organizations with decision advantage equips them to deal with both an IT portfolio and threat landscape that continue to grow in complexity. While this paper imagines the industry's future demise, this is merely a thought experiment – and one intended to make a positive case for how the industry can improve.

BACKCASTING AS AN ANALYTICAL TECHNIQUE

Backcasting is an analytical technique that begins by developing an imagined future scenario or outcome, and then works backwards to identify the hypothetical policies, variables, or events that caused that outcome. It is fundamentally different from forecasting, which instead seeks to predict a future as accurately as possible based on available known variables. Backcasting, by contrast, is not predictive. The imagined futures created can even be intentionally unrealistic. Its utility is instead to serve as a brainstorming exercise, i.e. if x were to happen (no matter how likely), what would be the likely reasons?

Backcasting has a variety of use cases. Businesses might perform backcasting exercises to imagine their circumstances in ten years' time. This could include scenarios where they are a market leader, or conversely, have gone bankrupt. This would then facilitate discussions around what might be the major causes of their imagined success or demise. This helps organizations to identify key pain points. For example, a lack of collaboration between different business units might be a major factor highlighted in a business collapse scenario. While the future scenario and the reasons that caused it are imagined, they inevitably shine a line on existing truths and lead to actionable takeaways (in this case, improving communication between teams).

Similarly, many government leaders would have no doubt learned valuable lessons in 2017 had they taken the time to backcast a hypothetical badly handled future pandemic with a high death toll. This could have helped to identify the key measures required before an outbreak occurred in real life. Indeed, one advantage of backcasting is that creating an imagined future scenario solicits an emotive response among participants that can help drive change.

Backcasting is used in various forms within cybersecurity, and has exciting potential to be applied further. Cyber crisis and tabletop exercises represent a form of backcasting. Participants will orchestrate a response to a plausible attack scenario. Wrap-up sessions will often review weak points in an organization's defences that could lead to a network compromise and help to improve security in key areas.

The approach also has untapped potential to be integrated with CTI. As highlighted by Rob Dartnall (Figure 1), backcasting can be used to imagine a future cyber attack conducted by an actor known to pose a legitimate threat to an organization. Information on their known tools, tactics, and procedures (TTPs) can then be plugged into the scenario. Backcasting exercises can therefore delve into attack vectors most likely to succeed.

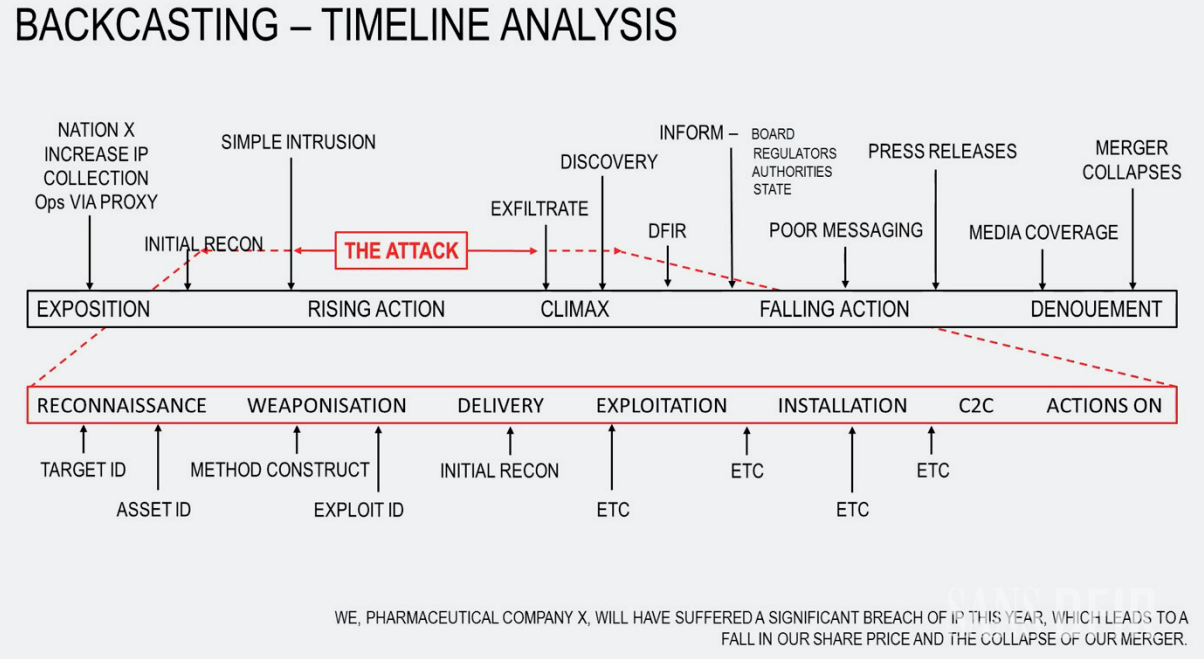

Figure 1: Backcasting a hypothetical cyber attack, integrating both TTPs and business impacts [1].

Rather than imagining a future attack, this paper applies backcasting to CTI by creating an altogether different scenario: the demise of the CTI industry itself.

BACKCASTING THE TURBULENT 2020s

The following section outlines the story of the Turbulent 2020s. The decade witnessed several dramatic shifts in the CTI industry. At this point it is worth stressing that as a backcasting exercise, this is not intended as a prediction and a large dose of creative freedom has been allowed.

2023: A maturing market

2023 showed encouraging signs of a CTI industry on an upward trajectory. CTI was now an established cybersecurity discipline and featured in the vast majority of organizations' security posture – whether through vendors or internal teams. The industry also proved remarkably resilient to broader economic shocks and continued to grow, often outpacing other cybersecurity functions.

Investors were increasingly eager to fund CTI ventures as a result of the industry's success. This enabled a string of youthful start-ups to emerge in the early 2020s. Fortunately for them, this was a relatively straightforward process as venture capitalists rarely bothered to verify their claims or scrutinize their market projections. Instead, after merely seeing that CTI was included in their pitch deck, the dollar signs in their eyes lit up. They were ready to part with their money.

An increasing number of CTI certifications and professional bodies had also begun to appear by 2023. The industry was therefore starting to converge around a common understanding of what constituted CTI and best practice.

2025: The champagne years

2025 was a happy time for those in the CTI industry. Multiple CTI vendors enjoyed seismic IPOs that made their way onto the front pages of the *Financial Times* and *Wall Street Journal*. CTI CEOs had become established public figures within the technology industry and were frequently invited onto flagship news programmes.

Among the champagne, parties and recently purchased yachts, the industry had also significantly matured. CTI professional bodies went on to become fully chartered. CTI analysts would take qualification exams by default, in a similar way to other industries such as accounting, law and auditing.

There were, however, quiet whispers among financial speculators that the CTI market could be in a bubble. A *Financial Times* opinion article was published, titled 'Have we reached peak CTI?'. Yet, any concerns around the industry's health were quickly dismissed by industry insiders. There was no time to be worried about bitter speculators who were simply jealous of their success.

2028: Market decline

The doom mongers of 2025 were soon vindicated as 2028 saw a steep decline in the CTI market. A global recession showed that CTI was as vulnerable to economic shocks as any other industry.

Many IPOs were delayed after anticipating a sceptical market would be unwilling to pay at their desired price. After signing multi-year contracts at the height of the industry's glory days, many end-users now began to question whether they should renew CTI services. While their cybersecurity budgets had not shrunk in the intervening years, CTI had not provided the value that they had hoped for. Many of these firms decided to allocate CTI budgets to other cybersecurity services and functions.

2030: The collapse of an industry

By 2030, the CTI market had all but collapsed. Most CTI analysts had at this point transitioned to other security functions, including digital forensics, incident response, and risk management. Website domain registrations for the major certified industry bodies and accreditation exams had, by now, expired.

A group of now-unemployed CTI veterans arranged to meet up for a final goodbye. The glory days of 2025 were now a distant memory. Among the stress and pressure of a declining market, the ensuing five years had not been kind to the majority in the room. A former CTI CEO stood up from the crowd. The pizazz and confident élan he had gained from running a multinational company was nowhere to be seen. Instead, now in a timid and self-conscious tone, he asked the room, 'How did it come to this?'

DISSECTING THE CRASH

The CTI industry collapsed due to a variety of reasons that are outlined in turn below.

Intelligence in isolation

The insular culture within many CTI teams was one key driver of the industry's decline. Many analysts were primarily focused on impressing the CTI community, rather than their employer or clients. Research was often done for the sake of research, the primary intention being for analysts to showcase their own talent and skills. Whilst this earned plenty of kudos at CTI conferences, its wider contribution was less clear.

By 2030, CTI teams were largely siloed from other cybersecurity processes and they typically operated as a stand-alone function. Well-written threat intelligence reports would be produced on a variety of topics, yet the audience of these reports was not clearly formulated. CTI teams were not asking how they could complement the work of those working in their organization on vulnerability management or within security operation centres. The lack of connection with other teams meant that the purpose of CTI function became difficult to grasp. In addition, while CTI could provide a positive return on investment, most CTI teams were uninterested in exploring the metrics or methodologies required to demonstrate this. Threat intelligence was therefore increasingly perceived as a luxury product, and one many businesses felt they could manage without.

CTI also isolated itself from other business units outside of the cybersecurity team. This led to missed opportunities for CTI to become embedded in highly strategic organizational functions. Risk management teams, who explored everything from the outlook of entering a new market to the hazards of outsourcing manufacturing, were not even aware that their organization had a CTI team. This was despite the clear contribution that CTI analysts could make by providing subject matter expertise on the cyber threat landscape within a new country or related to third-party exposure.
Analysts working for vendors also isolated themselves from business problems. Analysts were focused on writing reports. Although this was their primary responsibility, they failed to appreciate the wider context. This included issues around major client pain points that needed resolving, an understanding of where their business was heading, or the most frequent product requests that would help to attract and retain customers.

Distorted threat landscape

Whether consciously or not, CTI vendors failed to accurately portray developments in the threat landscape during the 2020s. Rather than a lack of foresight or a failure to anticipate nascent threats, the majority of the industry's failure was caused by exaggerating the threats that organizations and societies faced.

Much of this problem was caused by the industry's approach towards media and press engagements. In an attempt to increase their media coverage, the community naturally emphasized the most cutting edge and interesting attack vectors. This meant that commentary on the threat landscape placed a high premium on novelty: attacks embedding artificial intelligence (AI), deploying flashy zero-day exploits, and using niche MITRE ATT&CK tactics therefore gained a disproportionate amount of attention, despite their rarity [2]. Novel attack vectors were also at the forefront of the by then well-played-out January tradition of providing security predictions for the year ahead.

The problem with these narratives, however, was that they typically failed to resonate with the ground truth of most organizations on the ground. In 2027, rather than AI-enabled cyber attacks, organizations were still grappling with phishing and attacks targeting *Microsoft Office*. Organizations were looking for threat intelligence to help them prioritize patches, feed into their security operation centre, and identify strategic trends that could be integrated into their organization's broader risk strategy. Although less glamorous, organizations were most interested in many of the recurrent and often monotonous threats.

Just as media engagements over-emphasized novelty, the threat landscape was also distorted through sales cycles that played on fear. CTI pitches frequently overemphasized the threats posed to prospects. This was typified when a small 80-employee chair manufacturer invited multiple CTI vendors in to pitch their services, all of whom suggested their organization was likely a high-priority target for multiple state operations emanating from China, Russia, Iran and North Korea.

The notion that organizations had not yet woken up to the importance of cybersecurity might have held some truth in the mid 2010s, but by the early 2020s the situation had changed rapidly. If anything, the early 2020s had seen an overcorrection. Instead of neglecting cybersecurity, organizations now took it seriously on the whole and were arguably too ready to push the panic button. In such a shifting context, exaggerating threats became counterproductive.

What organizations increasingly needed was perspective, and a CTI function that could pick out tangible problems from the noise. Stoking fears helped to win clients initially, yet it meant that business relationships were built on hollow foundations. The discrepancy between the threat overviews presented on a pitch deck and the reports eventually sent to clients using empirical data meant CTI services were rarely renewed.

The threat landscape was also distorted through analysts' focus on their own pet interests. A large proportion of CTI analysts came from signals intelligence agencies and the military. This naturally led to an unconscious bias for analysts, who wanted to explore topics close to their heart.

Talent shortage

By 2030, it had become abundantly clear that the CTI community had failed to overcome the industry's chronic skills shortage. This had a dramatic effect on the quality of work being produced. Without enough people, under-resourced CTI inevitably missed warning signals, made mistakes, and took shortcuts. The lack of qualified CTI analysts also drove up the price for both talent and cybersecurity services. Robust security became unattainable for too many and added to a perception that CTI was a non-essential luxury for end-users.

The skills shortage also took a toll on those working within the CTI industry. Over-stretched analysts struggled to maintain a sustainable work-life balance among an ever-growing pile of intelligence requests. A 2030 study therefore concluded that the skills shortage was one of the most significant contributors to burnout and mental health issues within the CTI industry.

The CTI skills shortage was largely caused by three factors. First, the industry's recruitment efforts were too focused on narrow technical disciplines. Job descriptions frequently required reverse engineering and malware analysis skills. These were certainly important skills, yet by the end of the 2020s it had become increasingly clear that expertise in areas as disparate as social science, law and history could all make a contribution to the field. The industry therefore failed to foster a diversity of skillsets.

Second, the private sector was far too passive in fostering talent. While CTI vendors urgently needed qualified recruits, the cybersecurity skills shortage was largely perceived as a government problem. Rather than training their own analysts, security firms waited for CTI skills to be integrated into education programmes that never arrived.

Third, various non-profit organizations were unable to sustain their important efforts in developing skills and knowledge. From getting more women into the field to helping military veterans transition, a wide array of non-profits proved an essential component in both increasing and diversifying the talent pipeline. Initiatives such as The Many Hats Club fostered a thriving community that helped people find their first CTI job, while SecJuice provided a writing platform for new talent to find their voice and showcase their interest in CTI ahead of job interviews. For all these positive developments, however, the cybersecurity community never had a serious discussion about the role of non-profits or acknowledged the important way that they opened the industry up for new talent. As such, these vital initiatives did not receive an adequate level of investment.

Market conditions

Save a worldwide pandemic, there were plenty of other market conditions that disrupted the CTI industry.

The 2020s witnessed a rise of non-Western CTI vendors, appearing in regions ranging from China and Singapore to Israel and Oman. This created a more crowded marketplace and drove competition between firms. Non-Western vendors also often brought unique and different approaches. Many would focus on highly localized issues and covered the threat landscape within their own region in significant depth.

Generalist CTI firms also faced increasing competition from specialist vendors. These firms developed deep subject matter expertise on specific sectors, whether that be industrial control systems or telecommunication infrastructure. Although

specialized firms had a more restricted customer base, they became an attractive alternative for their target audience given their focus on a narrower set of highly prescient problems and threat developments.

MITIGATING THE FALL OF CTI

Although the above doomsday scenario might be unlikely, there is at least a grain of truth to many of the hypothetical problems outlined. The intention of this paper is to both bring attention to potential pitfalls within the CTI industry, but also crucially consider how they could be addressed.

The following section outlines actionable steps that can be taken to improve both the perception and value of CTI. Rather than a magical elixir of the industry's problems, it is hoped that identifying areas of improvement will help to elicit a broader conversation around the future direction of the industry.

Provide practical advice in marketing and intelligence reports

At its core, the CTI community should be focused on delivering value for organizations and intelligence consumers. One way to achieve this is through a remorseless focus on the 'so what' of both intelligence reports and external content. There is nothing inherently wrong with CTI content gathering press interest, yet researchers should also make sure that published content helps to inform and educate. Rather than research for its own sake, content would benefit from outlining relevant insight: i.e. the sectors and geographies that are likely to be most impacted, the future outlook, etc.

CTI organizations can help consumers even further by including practical advice and actionable steps to take. Mitigation advice against a reported attack vector, mapping against industry frameworks, or providing relevant indicators, can all help intelligence consumers to take action against the threat at hand. Critically, a call to action through practical advice is significantly more helpful than prompting a response by stoking fear, uncertainty and doubt.

It is also increasingly important for CTI functions to provide perspective over panic. There is now no shortage of threat vectors that organizations are worrying about. Yet, between phishing and fileless malware, AI-enabled offence and quantum-powered attacks, these different attack vectors pose radically different levels of relevance. CTI functions can play a vital role in helping organizations prioritize.

As organizations begin to take cybersecurity more seriously, the role of CTI should shift. It might at one point have been appropriate to mention the 200-plus potential threats an organization could face if their leadership team refused to accept that cybersecurity represented a serious business concern. However, as time goes on this will become an increasingly outdated viewpoint. For the increasing majority of organizations that do take security seriously, it is not helpful the belabour a long list of potential threats. Instead, the 10 attack vectors that are most likely to occur and that pose the most severe threat to their business strategy is the key insight required. CTI functions might therefore find one of their biggest contributions actually comes through downplaying threat vectors that pose a lower threat to organizations.

Adopt a collaborative approach

Rather than developing intelligence in a siloed and insular manner, CTI teams should work closely with other cybersecurity functions. Integrating CTI can often be achieved through building fusion capabilities that bring different cybersecurity functions together. Likewise, information sharing and analysis centres can facilitate industry-specific cooperation. These initiatives, however, require meaningful and active participation in order to succeed.

CTI teams should also work closely with intelligence consumers to understand what they are looking for when it comes to intelligence and how their services can be as useful as possible. Good listening skills are therefore a vital, yet too often neglected, skill for intelligence analysts. Gathering feedback should be an important component of any intelligence lifecycle. Almost all CTI functions would benefit from actively engaging with their intelligence consumers to determine whether the intelligence produced is useful and matches expectations.

CTI functions must also integrate feedback effectively. An agile culture is required to respond to shifts in demand and to produce intelligence relevant to stakeholders. Understanding consumer requirements will also likely mean different messages and delivery methods will be required for different stakeholders and client-bases. Different departments, geographies and sectors will likely require forms of intelligence based on their specific context and the threat landscape in which they operate.

The industry currently excels at writing detailed and thoughtful reports, yet much less attention is placed on how and whether these are effectively consumed. Feedback around intelligence should therefore be a two-way process. As well as soliciting feedback from customers, CTI functions should examine how intelligence is digested and provide consumers with feedback on how they can improve. This is particularly important given that CTI is still a relatively new industry, with its value and contribution likely unclear to some. Many organizations therefore have the potential to improve their ability to consume intelligence and integrate it across a wider variety of functions. An organization that subscribed to an intelligence service to aid their incident response posture, for example, might be missing opportunities to integrate services that they have already paid for into their vulnerability management processes, strategic risk management calculations and penetration testing.

Intelligence capability development [3] should therefore become a key pillar of CTI alongside intelligence production. This has the added benefit of creating a more symbiotic relationship between CTI teams and other business or cybersecurity functions: business will gain from the advice on how to better integrate and consume CTI, while this in turn makes CTI functions more useful and valuable.

Related to the above, intelligence should strive to be as integrated as possible with other aspects of cybersecurity and business strategy. Intelligence can feed into a variety of processes ranging from risk calculations to vulnerability management. Intelligence ultimately becomes more useful and sticky within cultures where it speaks to a variety of processes and contributes to solving multiple business problems. Above all, this requires a collaborative culture within CTI teams. CTI leaders need to build relationships with other areas of an organization, and understand how they can work together effectively.

Embrace intelligence as an educational tool

CTI functions should embrace their role as educators across an organization, including those largely ignorant about cybersecurity. The cybersecurity community is highly rigorous and security solutions based on bogus marketing claims are quickly chastised by the community. In many ways, this level of rigour should be celebrated: it highlights the industry's credibility and prevents dubious security solutions from spreading. Yet, the community's rigorous culture risks creating an overly hostile environment and almost snobby mindset among security purists. Too often, this level of rigour is turned back on those asking innocent questions. Those asking questions about issues and threats that are not perceived as valid are too often dismissed. While it is important to call out fear-peddling, there are also risks of dismissing valid and legitimate questions from those ignorant about cybersecurity.

For instance, it is plausible that a senior executive ignorant about cybersecurity could become concerned about the threat posed by AI-enabled quantum computing after reading a clickbait article from an untrusted source. As AI-enabled quantum computing is not deemed to pose a significant near-term threat by the vast majority of the cybersecurity industry, it would be all too tempting for CTI analysts to discount intelligence requests on the topic – perhaps even via a terse and dismissive reply. Yet, doing so would fundamentally misunderstand and underestimate the role that CTI can play in these situations. This is because a CTI function can arguably have a much more significant and disproportionate impact through educating those ignorant on cybersecurity, especially when they are senior decision makers. It is here that there is the most significant potential to dramatically increase cybersecurity understanding in a short time period. By contrast, although intelligence requests from so-called 'mature' consumers will likely lead to important mitigation steps being taken, there is a natural diminishing return in improving the knowledge of those who are already well informed about cybersecurity. A senior executive that is worried about a non-existent threat could still be in a position to divert significant resources towards addressing an imagined problem. CTI teams can therefore play a vital role in educating those ignorant about cybersecurity, focusing minds on tangible problems, and ensure that cybersecurity investments are aligned to the threats at hand. Crucially, CTI teams should not just tolerate stupid questions, but embrace them.

Building the pipeline

Despite the high number of cybersecurity vacancies, too many still require multiple years of experience. Organizations can, therefore, take more significant leadership on the issue by taking on and training new joiners [4].

One way firms can help to address the cyber skills shortage is by opening up entry-level pathways, whether that be apprenticeships for school leavers or internships and graduate schemes for university students. This would allow fresh faces to learn the fundamentals of cybersecurity on the job. By building their own pipeline of talent, CTI functions would address both their own individual staff requirements and contribute to fixing a broader problem within the cybersecurity industry.

One only needs to look at the various unusual journeys into the industry to realize that the industry is an eclectic bunch – one that welcomes those that haven't graduated high school and that come from unconventional backgrounds. A range of skill sets can, and do, contribute to the cybersecurity and CTI community. At the same time, however, this open-minded culture is not always reflected in job vacancies that often focus on a narrow set of technical skills. Organizations, therefore, have the opportunity to provide alternative formal pathways and career tracks, which utilize the skillsets of those from all walks of life (including the social sciences, humanities and arts).

CTI firms can also do more to communicate what they are looking for in new hires transparently. University careers advisers have no shortage of guidebooks and flashy PDFs to throw at students embarking on a career in law, banking or consulting. Unfortunately, the same cannot be said for a CTI career. It is, therefore, incumbent on cybersecurity firms to provide better guidance for future talent. This could include reading lists, resources for skills development, and information that can help to clarify possible career roadmaps for young talent. Mentorship is hugely important in the industry, and firms can play a role in facilitating this.

CONCLUSION

Both the 2030 market collapse and the causes behind it have varying degrees of realism. This paper is neither intended as a prediction of what is to come, nor an assault on the industry's current status. Yet, whilst a 2030 doomsday scenario is highly unlikely, the trends and issues discussed above should be taken seriously.

It is vital that the CTI industry guards against complacency. The cybersecurity market has enjoyed consistent growth, yet it remains a nascent industry. Its dynamics are still being determined. This makes working in cybersecurity incredibly exciting, yet it means the eventual shape of the industry remains uncertain. Predicting the role of CTI in ten years' time is difficult. Industry standards and a shared understanding of best practice are still being defined. CTI could go on to become indispensable to any serious cybersecurity function, yet its utility could also be underestimated and misunderstood if managed incorrectly. At the core of a successful CTI industry is a focus on delivering value for intelligence consumers. In this regard, the requirements are no different to intelligence requirements from 100 years ago: providing accessible, relevant and actionable intelligence.

The cybersecurity community must work hard to manage how CTI is perceived. This goes beyond a marketing issue, to one concerned about the industry's reputation as a whole. Even if the vast majority of CTI companies adopt best practice, a small handful of organizations could still tarnish the industry's reputation. There is already a perception within some circles that CTI is not intelligence at all, but simply data feeds vomiting irrelevant indicators. The CTI community must therefore take a proactive approach in shaping the industry's perception.

It is also vital that the CTI community embraces a highly reflective culture. Discussions around what best practice looks like, where the market is heading, how CTI is perceived, and potential industry pitfalls should all be a regular feature in research initiatives and conference proceedings. Industry bodies can continue to play an important role in facilitating these discussions, and drawing on the expertise across the entire community and vendor space.

As a cybersecurity function hyper-focused on assessing the threats and risks that organizations face, the CTI community would do well to apply this line of inquiry into their own industry.

REFERENCES

[1] Dartnall, R. Conventional Intelligence Analysis in Cyber Threat Intelligence – CTI Summit 2017. https://www.youtube.com/watch?v=jzHw8lkocXA.

[2] Collier, J. A Threat Intelligence Analyst's Guide to Today's Sources of Bias. Collier Jam. December 2019. https://collierjam.com/a-threat-intelligence-analysts-guide-to-todays-sources-of-bias/.

[3] Intelligence Capability Development. FireEye. https://www.fireeye.com/solutions/cyber-threat-intelligence/intelligence-capability-development.html.

[4] Collier, J. The Cybersecurity Skill Shortage Goes Beyond a Government Responsibility. Collier Jam. January 2020. https://collierjam.com/the-cybersecurity-skill-shortage-goes-beyond-a-government-responsibility/.