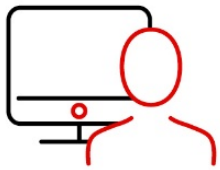
Mandiant

INTEGRATING INTELLIGENCE IN CYBER DEFENSE COMMAND AND CONTROL



This article focuses on the cyber defense function: **Command and Control** – how threat intelligence can influence your organization's decision-making, resource management, communications, and overall cyber security strategy.

Read Time: 7-10 Min

Command and Control is a common military term. In conventional warfare, Command and Control, or C2, is about how a commander directs their forces to achieve the mission. Think of "Command" as the strategic, decision-making aspects, while "Control" typically encompasses the operational aspects: what it takes to deploy capabilities and direct forces to achieve mission objectives.

For our purposes, C2 is any function or entity that directs or coordinates capabilities of the cyber defense mission. In short, the C2 function ensures everyone is rowing in the same direction.

How should we develop our Command and Control function, and how should it use threat intelligence? The answer to the first part of the question depends on your organization. For example, how command and control is actualized in cyber defense can be very different at a regional bank than at a national-level cyber security agency. The key differentiators are the scale and scope of the mission (what you are trying to defend and why), the resources you have available, and your threat profile.

The second part of the question is easier to answer but requires us to explore more detailed concepts. Despite differences in the development of command and control functions between organizations, there are many commonalities in how those different iterations leverage threat intelligence.

Maintaining the Mission with Command and Control

In collaboration with the larger information security program, the Command and Control (C2) function prioritizes cyber defense resources to protect the organization from threats with the highest likelihood of impact based on Intelligence.

NIST has a **definition in their Computer Security Resource Center (https://csrc.nist.gov/glossary/term/command_and_control)** for C2. The Congressional Research Service also has a **defense primer on C2 (https://sgp.fas.org/crs/natsec/IF11805.pdf)**, and provides a summary of its concepts.

We'll look at these commonalities, and at the steps you can take to have a well-integrated Command and Control function that harnesses intelligence.

Objectives and Key Actions for Application

From Mandiant's observations and direct support in building customer intelligence capabilities, managing cyber threats and their related risks are much more likely to succeed when intelligence is integrated into the main aspects of C2. This particular integration works best from both strategic and operational perspectives. Accessing and providing good intelligence during an incident or breach is important, and this may be your top concern. Communicating strategic intelligence to organizational leadership can have equal value, empowering them to make important long-term decisions that proactively reduce risk over time. The recommended intelligence applications that follow are organized around fundamental strategic and operational activities typically associated with a C2 function.

C2 Application #1: Threat Communication and Cross-Functional Coordination

One of threat intelligence's core value propositions is assessing the risk of imminent threats and driving actions to proactively protect users, data, and systems. To do this effectively and repeatedly, the C2 function's role when communicating intelligence is paramount. Beyond effective communication, C2 activities can use intelligence when coordinating activities across various functions in your organization. What follows are some key activities to support these goals.

Implement operational workflows that identify and communicate high priority intelligence

When a threat is emerging or imminent, intelligence needs to flow to the right shareholders at the right moment. Often in these cases, we can't wait for full, in-depth analysis before action must be taken.

One Intel Report, Many Uses

One critical value of the C2 function is to act as a central clearing house for important, actionable intelligence. As an example, consider the intelligence needs of a national UK courier company who rely on centralized databases to sort and deliver packages to clients. If the C2 function received reports of a ransomware that is targeting courier companies, there are several important shareholders who would need to be made aware prior to any further activity. These may include:

- The internal team responsible for managing the centralized database at risk
- The Executive responsible for customer service
- The SOC, detection and mitigation teams

In this instance, the C2 function can ensure every necessary shareholder receives the initial intelligence and coordinate questions on further steps being taken.

Prior to a more extensive analysis, intelligence deemed high priority or high impact needs be quickly communicated. How it is communicated is sometimes easy to overlook. Good intelligence shouldn't create panic or confusion. Intelligence should be formatted and disseminated based upon the relevance to the organization, the needs of specific decision makers, and in a modality that achieve these results consistently across all shareholders.

For effective C2, it's not just about communication. It's also about coordinating efforts symphonically across different teams in the organization, relying on good intelligence to help make that happen whenever possible. Having a cyber threat profile developed and regularly updated will make this task more efficient, in addition to having well-defined intelligence requirements and shareholder needs established and understood by those performing C2 roles. Those roles should have deep insight into which shareholders can take different types of action based on a variety of threat scenarios and the intelligence they are provided with. We are trying to route the most pertinent and actionable intelligence to the

right people in as little time as possible, but with the proper intent, purpose, and clarity.

Implementing these workflows and practices takes time; developing, testing, tuning, and integrating them across existing teams in a collaborative way can be resource intensive. As part of this, the C2 function, with the support of senior leadership, can cultivate a common understanding of the cyber threat profile, the different types of intelligence deemed vital across different shareholders, and what actions should be taken by individual functions and the organization at large.

Institute strategic workflows that support risk reduction

Many organizations remain focused on recent or near-term responses to threats. Tactically and operationally focused teams rightly need to concentrate on defending against active threats, or those likely to emerge in the near-term.

When not in that reactive "crisis mode," intelligence related to nascent threats should be balanced by strategic intelligence, especially the analysis of trends relevant to your organization. In this regard, the C2 function is often expected to:

- Understand new trends emerging in the broader threat landscape that are relevant to them.
- Determine when significant changes to threat trends affect their exposure and potential impacts.
- Understand how persistent threat trends will continue to affect their defensive posture over time.
- Identify and produce technical and operational recommendations to different teams in the organization that will limit exposure to evolving threats.
- Coordinate actions resulting from the points above and provide recommendations or insight to risk functions.

By supporting the organization in these strategic aspects, the C2 function can gain important visibility and insight into risk-based decisions. Understanding how evolving threats affect these different risk equations can be complex, but the C2 function should help deconflict and coordinate this effort across your organization, enabling accurate and timely risk assessments. This can cause a positive ripple effect, amplifying the value of threat intelligence. Having insight into these decisions and the residual risk can help maintain longer-term readiness of operational teams. If the C2 function understands what longer term risks may impact the organization most, they can help manage resources more strategically and enhance preparedness.

Collect shareholder feedback from internal reporting and recommendations

As a matter of course, intelligence providers should solicit or monitor for feedback on reporting, analysis, and recommendations provided. While analysts are often best placed to request feedback, given they often serve as a point of contact for the delivered intelligence, the C2 function has an important role in coordinating the overall role feedback can play in downstream intelligence activity. The C2 function can aggregate this feedback, document it , deconflict any misinformation with shareholders, and manage those action items-keeping the Intelligence function focused on the threat. C2 can also:

- Include findings and recommendations within metrics and reporting on the effectiveness of the intelligence program.
- Determine points of irrelevancy to eliminate unnecessary intelligence activity.
- Determine under-performing areas of intelligence activity that require further attention.
- Measure the competency of the Intelligence function within the program.
- Pivot and iterate the foci and intent of the intelligence program.

Specifically for the intelligence function, action items can include additional research, collection of new information, or re-analysis of existing intelligence.

For example, feedback on intelligence reports collated by the C2 function can identify that a shareholder is seeking less information on Topic A and more on Topic B. The C2 function can then interact with various elements of the intelligence program to ensure efforts against Topic A are reduced and those against Topic B are prioritized and increased.

The most obvious application of this example is the C2 function ensuring the organization's intelligence requirements are accurate, feasible, effective, and drive downstream intelligence activity.

C2 Application #2: Influencing Cyber Defense Strategy

There are many ways and opportunities to influence an organization's overall strategy with intelligence. These opportunities present themselves at different times and can originate from many different sources (various internal functions or external entities like consultants, government agencies, or auditors). One of the challenges we've tried to help our customers solve is how intelligence can influence their strategy in a repeatable, programmatic way, and in a manner that has a lasting and measurable positive impact.

If your C2 function has the visibility and insight into what is working or not working across an entire cyber defense program, it stands the best chance at helping to solve this. Here are some recommended activities your C2 function can regularly perform to ensure you are getting the most strategic value from intelligence.

Perform a comparative analysis on the organization's threat profile against your cyber defense strategy

C2 roles can collaborate with senior leadership and shareholders, analyzing significant threats to the organization against the mission scope, priority objectives, functional resource allocations, capability enhancements, and other investments. At a high level, the C2 function and leadership elements within the organization should be able to compare these priorities and determine if they are well-aligned to relevant cyber threats. A comprehensive and current threat profile can really help with this analysis. The threat profile should help to understand adversary motivations and intent, aiding in identification of threats to reputation, mission, services, assets, or personnel. Adjusting the organization's cyber defense strategy and policy translates this understanding into action.

Re-align your strategy by recalibrating program policies

Once you know what strategic adjustments you need to make, you can start to orchestrate these changes. In the most general sense, program policies are used to establish and drive an organization's cyber defense program based on a well-defined strategy. Leadership issues or changes program policy when strategy and priorities change. They define the purpose of the program and its scope within the organization, basic goals per function, and assignment of responsibility across the organization (derived from NIST Special Publication 800-12 Revision 1).

In other words, program policies keep things on the rails, ensuring strategy is realized operationally by establishing the responsibilities, rules, actions, and expected outcomes of various functions. When changes are made, this can spawn new initiatives, projects, and investments. Resources needed to achieve strategic objectives are then identified. It's a process to say the least, requiring lots of cross-functional collaboration and a support network of experts that really understand the mission or business and how to get things done within the organization.

Provide intelligence support to strategic initiatives

Once the strategic direction is adjusted and reflected in changes to program policy, the stage is set for minor, moderate, or transformative change within your organization. The C2 function can leverage the cyber threat profile and other key intelligence to consistently align resources, investments, and projects against relevant cyber threats.

Working with program and project managers on cyber defense initiatives, and providing them with intelligence to support their goals, can be key to ensuring the strategy is realized. Since the cyber threat landscape can rapidly change, it is important to keep key intelligence flowing and in the hands of those driving this important work. This provides

shareholders with a greater insight into how their initiatives align to the threat landscape and can help expedite transformation by promoting a threat-focused approach.

When threats emerge or evolve, adjustments may need to be made to these projects or initiatives. An example of this would be the discovery of a new tactic or technique threat actors are leveraging. Perhaps a new technical security control is being implemented in your organization and may not detect or protect against it. In this case, you would want to get this intelligence to individuals managing this initiative and help advise on a course of action. It may even require working with the developer or the third-party vendor to ensure that there is appropriate coverage for the new technique.

C2 Application #3: Using Intelligence to Guide Security Policies

Security policies are important to ensure the safety, security, and consistent use and application of systems and data. Many security policies center around the misuse, abuse, or mishandling of systems and data, and are supported through enforcement measures against offending employees.

As intelligence is concerned with imminent or emerging threats to organization's systems and data, the C2 function has a central role to play with support to policy makers to enable better decisions focused on lowering risk. What follows are some activities that might help with this decision making.

Inform security policies with Threat Intelligence

Issue-specific information security policies are developed to address areas of current concern to an organization. Their intent is to provide specific guidance and instructions on *proper usage of systems* to individual users within the organization. Evolving and emerging cyber threats affect how people securely use different technology needed to do their jobs. Issue-specific policies are written in such a way that this will be clear to users, and they can often be informed by cyber threat intelligence to reinforce the importance of the policy.

Intelligence on the capabilities of emerging threats that place the organization at risk can inform gaps or weaknesses in system-specific policies. System-specific policies provide information and direction *on what actions are permitted on a particular system*. These are like issue-specific policies in that they relate to specific technologies throughout the organization. However, system-specific policies dictate the appropriate security configurations to the personnel responsible for implementing the required security controls (see NIST Special Publication 800-12 Revision 1).

As a central coordination function, the C2 function can be best positioned to determine gaps or alignments needed across both issue and system-specific policies, as it pertains to meeting the strategic goals of the cyber defense program. Providing threat intelligence in this pursuit helps policy (and policy enforcement) align appropriately to threats.

Advise on insider threat policies

Cyber threat intelligence can also guide policy regarding insider threats. Mandiant defines insider threats as the abuse or misuse of corporate technology, assets, and/or information by those with privileged or trusted access. This often means employees, or any users with trusted access to your systems and data. Insiders with malicious intent can enact severe damage, given their knowledge of policies, systems, and how their organization may react to such abuse and misuse. Well-positioned and meticulous insiders can expose your organization to severe risk and reputational damage.

For these reasons, the C2 function should inform those functions responsible for establishing privileges and access permissions on the significant risks and potential impact of insider threats. The C2 function can also help system owners and risk managers calibrate the tension between maintaining secure systems and allowing sufficient privileges and access to enable business productivity.

Support security awareness programs

Similar to insider threat policies, cyber threat intelligence can have a major influence on the direction and success of

security awareness programs and policies. Security awareness is the internal outreach program that provides advice, guidance, and warnings to all end-users, regardless of their role or position with the organization. Security awareness programs are necessary to encourage the development of a well-balanced security culture that doesn't stifle business productivity but ensure all end-users take personal responsibility for their own conduct. The C2 function should collaborate with the security awareness function to provide guidance and direction based on relevant intelligence.

For example, email phishing remains one of the top attack vectors used by a variety of sophisticated and non-sophisticated threats. Without a culture of personal responsibility regarding security, the attack surface represented by email (incoming and outgoing) remains broad and deep. Security awareness policies should be written by those functions responsible for enterprise risk; however, they can utilize cyber threat intelligence to empower their policies and the resulting programs in several ways:

- The focus of security communications can be aligned with emerging or current threats to reduce exposure.
- The C2 functions can coordinate by providing succinct case studies or examples relevant to the security awareness program's monthly focus. Often a well-placed, recent example can reinforce the underlying security message.
- The C2 function can coordinate regular threat briefings with security awareness teams to appropriate business units to reinforce widely shared communications, or to focus on specific risks facing those business units whose core focus is not security-related.

Incident and Crisis Management

Some organizations may operate a broader incident or crisis management function in parallel to a more technical, cyber defense-focused incident response team. This may be a standing function with regular coordination, or it may only convene in the event of a major incident or crisis that impacts critical services, technology, and cyber risk.

This often represents a decision-making function comprised of leadership from a variety of core business, legal, security, communication, enterprise risk, and executive business units. These entities all represent potential intelligence shareholders, with both unique and overlapping requirements that are often determined by the nature of the incident, crisis, or scenario. The C2 function should work with these teams to ensure they know exactly what types of intelligence should be integrated into these larger organizational processes or playbooks.