
***What Does CTIIC Do?***

CTIIC **builds understanding of foreign cyber threats to US national interests** to inform decision-makers at all levels, including in federal cyber centers, departments and agencies, and senior policymakers.

CTIIC's mission responsibilities are outlined in a **February 2015 memo Presidential Memorandum** that directed the DNI to establish CTIIC to:

- Provide **integrated all-source analysis** of intelligence related to foreign cyber threats or incidents affecting U.S. national interests;
- **Support federal cyber centers** by providing access to intelligence necessary to carry out their respective missions;
- Oversee development and implementation of intelligence sharing capabilities to **enhance shared situational awareness**;
- Ensure that **indicators of malicious cyber activity and**, as appropriate, **related threat reporting** contained in intelligence channels **are downgraded** to the lowest classification possible **for distribution to both U.S. Government and U.S. private sector entities**;
- **Facilitate and support interagency efforts to develop and implement coordinated plans** to counter foreign cyber threats to U.S. national interests **using all instruments of national power**, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

CTIIC is an **advocate**: for addressing hard challenges, collaboration, information-sharing, a common lexicon, and other activities that position the US Government to understand and address cyber threat.

**Presidential Policy Directive (PPD) 41 on Cyber Incident Coordination** names CTIIC as one of three Federal lead agencies (with DHS and FBI) to coordinate the response to a significant cyber incident. CTIIC is the lead agency for intelligence support and related activities.

## QUICK FACTS

**Directed** by Presidential Memorandum

**Authorized** by Congress in the FY16 Intelligence Authorization Act

Scoped small to **support**

- > 80% detailees
- ODNI + 6 agencies

**Core Lines of Business**

- Build Awareness
- Integrate Analysis
- Identify Opportunity
- PPD-41 role

CTIIC does **not** do:

- Operations
- Collection
- Private sector

**CTIIC Advisory Board**

- Cyber Center chiefs and Cyber Intel executives
- Tackles common challenges

***Why Is CTIIC Needed?***

CTIIC is a **small, multiagency** center that works to increase the speed at which the US Government recognizes significant cyber activity is threatened or occurring so decision-makers can act to prevent or minimize damage to US national interests.

- It is an **integration point** where analysts scrutinize **fragments** of cyber threat information produced by network defenders, Intelligence Community, law enforcement, incident responders, and non-

Government sources; make connections; place the activity in context; call attention to significant activity; and work with partners to develop whole-of-government approaches to mitigate or counter the threat.

- CTIIC's products have become a "must read" for cyber and noncyber specialists wishing to understand the most current cyber threat reporting and the integrated **community assessment** of how our adversaries are using cyber means in support of their objectives.

ODNI and the agencies who produce cyber threat intelligence designed CTIIC so that it **supports,** but does not duplicate, the work of other centers and agencies. This group also defined what CTIIC does ***not*** do.

- CTIIC **does not collect**. It integrates and highlights information and expertise from around the community.
- It is **not operational.** CTIIC supports operators by ensuring they have the fullest possible threat picture, and that parties with a range of tools and authorities are at the table when decisions are made.
- CTIIC has **no direct liaison** with the private sector. It works through agencies who ***do*** have those relationships and helps to downgrade information and analysis they can share.
- The Center does not advocate a "CTIIC view." It produces **community analysis** on current threat issues by working with a wide set of experts (cyber, regional, technical, etc.) and by setting cyber activity in a broader context.

***What Are CTIIC's Main Lines of Effort?***

CTIIC **builds awareness, integrates analysis,** and **identifies opportunities.**

- ***Awareness.*** Awareness of our adversaries' threat activities is the first step needed to disrupt and mitigate its consequences. CTIIC builds awareness by integrating threat reporting with context to highlight its potential significance for decision-makers. CTIIC does this through research and engagement with other cyber centers and the producers of intelligence and analysis, including noncyber experts. This work builds understanding of threat activity, makes cyber reporting accessible to noncyber specialists, and is a building block for trend analysis.
- ***Integrated Analysis.*** The Federal cyber community has faced increasingly aggressive activity from adversaries that has demanded detailed and complex **community analysis on current and near-term threats.** This cyber activity can best be understood by analyzing it in the context of adversaries' capabilities, motivations, and intentions. CTIIC collaborates with cyber and noncyber subject-matter experts to initiate and integrate community analysis that considers threat activity in this context as a baseline for informing decisions on how to mitigate or counter the threat.
- ***Opportunities.*** CTIIC supports and facilitates **whole-of-government options** in response to cyber threats to help ensure decision-makers receive potential courses of action that reflect **all instruments of national power.** CTIIC delivers opportunity analysis and assessments of measures of effectiveness for cyber campaign efforts. The Center identifies ways to facilitate critical decision points and creates repeatable, threat actor–agnostic frameworks that balance risks, benefits, and equities early in the decision-making process.

***How Does CTIIC Ensure It's Supporting Its Partners?***

**CTIIC** hosts recurring meetings of an **Advisory Board** composed of leaders of the federal cyber centers and the significant producers of cyber threat intelligence. The Board has two purposes: to advise CTIIC on how best to support the community and to provide a forum for discussing solutions to shared challenges.


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu