Cyber Threat Intelligence Integration Center (CTIIC)

MISSION

Integrate cyber threat intelligence to inform national interests, support national cyber policy and planning efforts, and coordinate an IC-wide approach to cyber collection and investment.

HISTORY

On 11 February 2015, the Assistant to the President for Homeland Security and Counterterrorism announced the establishment of CTIIC under the auspices of the Director of National Intelligence. CTIIC was established as a result of the IC's lessons learned in responding to the 2014 cyber attack on Sony Pictures. CTIIC's responsibilities were codified in a Presidential Memorandum issued on 25 February 2015.

Today, CTIIC works closely with ODNI's National Intelligence Officer for Cyber, IC Chief Information Officer, and National Counterintelligence and Security Center to carry out its intelligence mission in coordination with the policy community.

PRIORITIES

Integrate Cyber Threat Intelligence

CTIIC integrates IC and commercial cyber intelligence to inform a variety of audiences from senior policymakers to network defenders. CTIIC also leads the IC's intelligence support to government incident response efforts.

Build Innovative Partnerships and Capabilities

CTIIC engages across the IC and US Government (USG) and with foreign and industry partners to increase visibility into cyber threats, enhance processing and sharing of cyber intelligence, incubate new cyber capabilities, and further the development of the IC's cyber workforce.

Guide IC Investment and Strategic Priorities

CTIIC collaborates with IC elements to identify opportunities to integrate cyber collection, data exploitation, and analysis across the IC and to align funding with national priorities.

KEY INITIATIVES

The **Cyber Response Group (CRG)** serves as the White House's primary vehicle for coordinating the USG response to cyber events with national security implications. Each week, working with the White House and USG counterparts, CTIIC identifies relevant and timely cyber topics and briefings to give stakeholders the intelligence they need to respond to cyber incidents.

Cyber Threat Intelligence and Event Reports
CTIIC produces the all-source Cyber Threat Intelligence Summary and Congressional Cyber Threat Intelligence Digest to keep USG stakeholders abreast of the latest cyber reporting. CTIIC's Cyber Event Report serves as the USG's coordinated intelligence product for summarizing major cyber incidents and capturing USG and private sector response activity.

Commercial Intelligence Partnerships
CTIIC engages with cyber intelligence companies to augment the IC's reporting of attack trends, track cyber threat actors, and inform key policy questions.

CTIIC hosts the **Cyber Strategy Board (CSB)** to synchronize IC agencies' cyber intelligence missions and develop coordinated strategies on major cyber topics and investments. Board members identify collaborative opportunities—including shared tools, analysis, and resources—to best serve an array of policy and defense customers.

CTIIC provides **integrated intelligence support to the National Security Council** policy process for topics related to cyber threats, cyber operations, and associated technologies—including support to whole-of-government efforts led by the Office of the National Cyber Director, Department of Homeland Security, National Cyber Investigative Joint Task Force, and others.

Visit our website at www.dni.gov/ctiic