United States Government Accountability Office

Report to Congressional Requesters

March 2023

GLOBAL CYBERCRIME

Federal Agency Efforts to Address International Partners' Capacity to Combat Crime

Accessible Version

GAO-23-104768

GAO Highlights

Highlights of GAO-23-104768, a report to congressional requesters

March 2023

GLOBAL CYBERCRIME

Federal Agency Efforts to Address International Partners' Capacity to Combat Crime

Why GAO Did This Study

The U.S. and its global partners are experiencing the effects of a massive cybercrime wave, which is growing in frequency and scale. In 2021, the Federal Bureau of Investigation received a record number of cybercrime complaints, over 840,000, with potential losses exceeding $6.9 billion. Further, in 2022, the intelligence community noted an increase in ransomware attacks by transnational criminals, which threaten to cause disruptions of critical services worldwide.

GAO was asked to review federal efforts to build the capacity of allies and partner nations to combat cybercrime. This report's specific objectives were to (1) describe challenges in building global capacity to combat cybercrime, and (2) determine actions selected federal agencies are taking to build foreign nations' capacity to combat cybercrime and the extent to which they are evaluating the effectiveness of their efforts.

GAO interviewed agency officials and convened a panel of experts representing entities focused on capacity building to combat global cybercrime. GAO also analyzed documentation from State, DOJ, and DHS, which provide the majority of U.S. capacity building assistance.

What GAO Recommends

GAO is making one recommendation to State to conduct a comprehensive evaluation of capacity building efforts to counter cybercrime. State concurred with the recommendation.

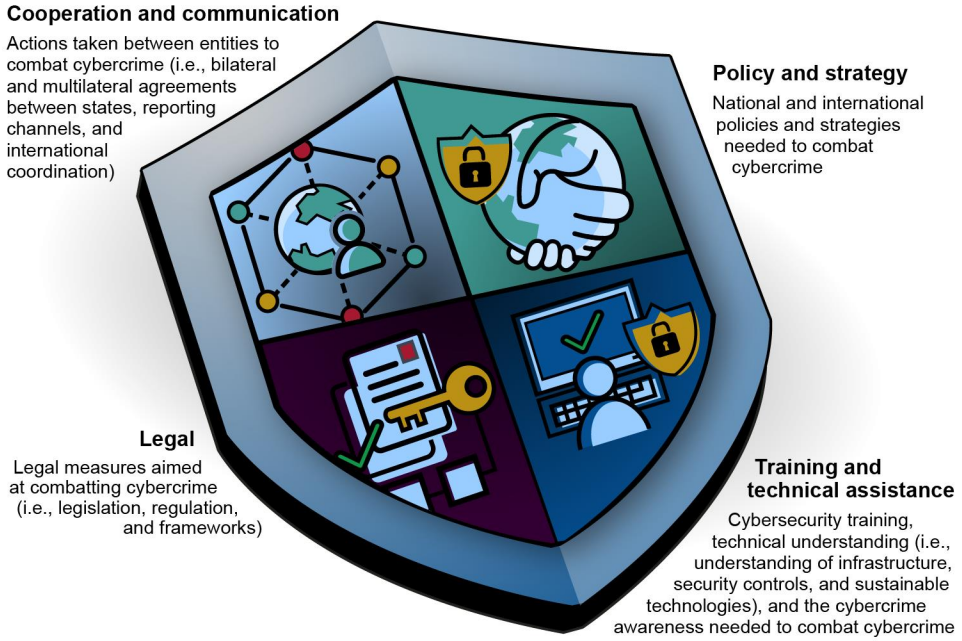
View GAO-23-104768. For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov or Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov.

What GAO Found

The Departments of State, Justice (DOJ), and Homeland Security (DHS) officials, and experts from international entities identified six mutual challenges in building global capacity to combat cybercrime. These included a lack of dedicated resources, difficulties in retaining highly trained staff, and inconsistent definitions of "cybercrime." The expert panel also identified challenges in working with the U.S. government, including obstacles in obtaining information, lack of collaboration, and lack of dedicated funding streams.

State, DOJ, and DHS have conducted a variety of activities to build foreign nations' capacity to combat cybercrime. These activities include engaging in information sharing with foreign partners and providing cyber training to foreign law enforcement officers. Agencies' activities can be grouped into four categories.

Four Categories of Activities to Build Capacity to Combat Cybercrime



Source: GAO analysis; image: Buffaloboy/stock.adobe.com. | GAO-23-104768

These agencies have documented accomplishments for many activities, such as nations joining international treaties aimed at combatting cybercrime. Further, State's plans include an evaluation of a regional forensics training center. This planned evaluation would meet the department's requirements. However, State has not conducted a comprehensive evaluation of the agencies' collective efforts. State is in the best position to conduct such an evaluation since it is authorized to provide foreign assistance funding to help build key allies' and partners' capacity to combat cybercrime. Until State conducts this comprehensive evaluation, the overall impact and results of federal assistance to global partners will likely remain unknown.

Contents

Figures

Abbreviations

CRM	Criminal Division
DHS	Department of Homeland Security
DOJ	Department of Justice
GLEN	U.S. Transnational and High-Tech Crime Global Law Enforcement Network
FBI	Federal Bureau of Investigation
ICE	Immigration and Customs Enforcement
ICHIP	International Computer Hacking and Intellectual Property
INL	Bureau of International Narcotics and Law Enforcement Affairs
State	Department of State

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 1, 2023

The Honorable Robert Menendez
Chairman
Committee on Foreign Relations
United States Senate

The Honorable Michael McCaul
Chairman
The Honorable Gregory Meeks
Ranking Member
Committee on Foreign Affairs
House of Representatives

The rapid increase in computer technology has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. However, it has also multiplied the potential power and reach that can be leveraged in committing crimes, affecting victims around the globe. Criminals exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, ransomware attacks, and intellectual property theft.

The U.S. and its global partners are experiencing the effects of a massive cybercrime wave, which is growing in frequency and scale. In 2021, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center[1] received a record number of cybercrime complaints, over 840,000, with potential losses exceeding $6.9 billion.[2] According to the FBI, these complaints address a wide array of internet-enabled scams affecting victims across the globe.

In addition, according to the United Nations, the complex nature of cybercrime is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime and their victims are often located in different regions, and its effects ripple through societies around the world.

You requested that we review the strategy and effectiveness of the federal government's efforts to build the capacity of allies and partner

[1]The FBI's Internet Crime Complaint Center provides the American public with a source for information on cybercriminal activity, and a way for the public to report when they suspect they are a victim of cybercrime.

[2]FBI, *Internet Crime Report* (Washington, D.C.: 2021).

nations to combat cybercrime. The specific objectives for this report were to (1) describe challenges in building global capacity to combat cybercrime, and (2) determine actions selected federal agencies are taking to build foreign nations' capacity to combat cybercrime and the extent to which they are evaluating the effectiveness of their efforts.

To address the first objective, we analyzed plans, strategies, and our prior reports to determine the key federal agencies that provide assistance to combat cybercrime. We selected the Departments of Homeland Security (DHS), Justice (DOJ), and State based on their specialized functions related to investigating and prosecuting cybercrime, and numerous global efforts that provide cybercrime support. Specifically, we determined that DHS's U.S. Immigration and Customs Enforcement (ICE) and U.S. Secret Service, DOJ's Criminal Division (CRM) and FBI, and State's Bureau of International Narcotics and Law Enforcement Affairs (INL) provide the majority of U.S. assistance in this area. We interviewed agency officials to gather challenges they face in building global capacity to combat cybercrime, compiled the identified challenges, and confirmed with each agency that they face each challenge in the resulting list.

We also convened a panel of experts representing entities that work to combat global cybercrime, including the Global Forum on Cyber Expertise, Global Cyber Security Capacity Center, and United Nations Office on Drugs and Crime, among others. During the panel, we gained panelists' perspectives on challenges they face in providing capacity building assistance to partner nations, and challenges they face in working with the U.S. government when providing assistance, among other topics. We provided DHS, DOJ, and State officials an opportunity to comment on challenges the panelists identified in working with the U.S. government.

To address the second objective, we analyzed various reports, such as the Council of Europe, *Global Project on Cybercrime–Capacity Building on Cybercrime*, and the United Nations Office on Drugs and Crime's draft *Comprehensive Study on Cybercrime*. We used these reports to help develop our definition of capacity building to combat cybercrime, and to identify categories of, and develop definitions for, activities to build capacity to combat cybercrime. We identified categories through research on the types of assistance entities provide to combat global cybercrime, and determined that assistance could be grouped into four categories. Next, we collected documentation regarding activities that DHS, DOJ, and State have undertaken to support efforts to build capacity to combat cybercrime and organized their efforts into our four categories.

We also analyzed the agencies' documentation to determine if there were any overarching strategies or whole-of-government programs that outlined their efforts. Specifically, we determined if they documented total funds allocated and spent on these efforts, processes for selecting countries to conduct these efforts, and comprehensive evaluations on overall efforts rather than individual activities. Additionally, we compared agency documentation against requirements established by the GPRA Modernization Act of 2010, including if strategic plans established goals that contributed to agency priorities as well as performance indicators intended to monitor progress towards goals. We compared State's outputs and outcomes against department-specific program evaluation requirements. A detailed discussion on our objectives, scope, and methodology is provided in appendix I.

We conducted this performance audit from January 2021 to March 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Numerous reports have highlighted cybercriminals' ability to cause greater disruptions of critical services worldwide, with low risk and high reward.[3] Ransomware ranked consistently among one of the most dangerous, disruptive, and costly occurring cybercrimes because of its ability to disrupt critical infrastructure, including government and health care facilities, as well as supply chains.[4] Among other frequently occurring cybercrimes were business email compromise, identity theft,

[3]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 7, 2022); FBI, *Internet Crime Report* (Washington, D.C.: 2021).

[4]For further information about ransomware and supply chains, see GAO, *Ransomware: Federal Coordination and Assistance Challenges,* GAO-23-106279 (Washington, D.C.: Nov. 16, 2022); and *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

and denial of service attacks on computer networks.[5] For example, the 2022 Annual Threat Assessment of the U.S. Intelligence Community noted that many major transnational cybercrime groups have diversified business models that engage in direct wire-transfer fraud from victims, or use other forms of extortion alongside or in place of ransomware.[6] It noted that in 2020, business email compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes.

State's INL Cybercrime Strategic Guidance also acknowledged ransomware as the most dangerous and disruptive method of cybercrime, and business email compromise and denial of service attacks on computer networks as other forms of frequently occurring cybercrime. In addition, the FBI's 2021 Internet Crime Report highlighted that among the 2021 complaints received, business email compromise schemes, ransomware, and the criminal use of cryptocurrency were among the top incidents reported. More specifically, in 2021, business email compromise schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion.[7]

Finally, DHS's Cybersecurity and Infrastructure Security Agency, the National Security Agency, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure entities globally in 2021.[8] They reported numerous growing behaviors and trends among cybercriminals, such as sharing victim information between ransomware groups, threatening to publicly release stolen sensitive data, and disrupting internet access.

International Conventions on Countering Cybercrime

The Council of Europe Convention on Cybercrime (known as the Budapest Convention) is the first international treaty on crimes committed

[5]Business email compromise is a scam that involves compromising email accounts to conduct unauthorized transfer of funds. A denial of service attack is an attack that prevents or impairs use of networks, systems, or apps.

[6]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 7, 2022).

[7]FBI, *Internet Crime Report* (Washington, D.C.: 2021).

[8]Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware*, AA22-040A (February 2022).

via the internet and other computer networks.[9] It is the most comprehensive international agreement on cybercrime and electronic evidence.

The Convention's main objective is to pursue mutual crime prevention aimed at protecting and defending society against cybercrime, specifically by promoting appropriate national-level legislation and fostering international cooperation. It also includes programs focused on capacity building. Specifically, countries that have acceded or requested accession to the Convention may become priority countries for capacity building programs. This is intended to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally. DOJ, in particular CRM and FBI, and State, in particular INL, play a large role in these capacity building efforts.

Additionally, in recognition of the growing cybercrime threat, in December 2019, the United Nations General Assembly set in motion a process to draft a new convention on countering cybercrime. It established an ad hoc committee to develop a comprehensive international convention. Further, the General Assembly was to take into consideration existing international efforts on combatting cybercrime. This included the outcomes of an intergovernmental expert group that conducted a comprehensive study on cybercrime and responses to it by member states, the international community, and the private sector, from 2011 to 2013.[10] Negotiations for the convention began in February 2022 and a draft convention is expected to be completed in 2024.

[9]In May 2022, the U.S. signed the Second Additional Protocol to the Budapest Convention, which aims to further enhance cooperation on cybercrime and electronic evidence sharing through more efficient mutual assistance tools and other forms of cooperation between countries, cooperation in emergencies, and direct cooperation between law enforcement in one country and service providers and other private entities in another country. As of February 2023, there are 68 Parties to the Convention, and 19 countries signed or invited to accede.

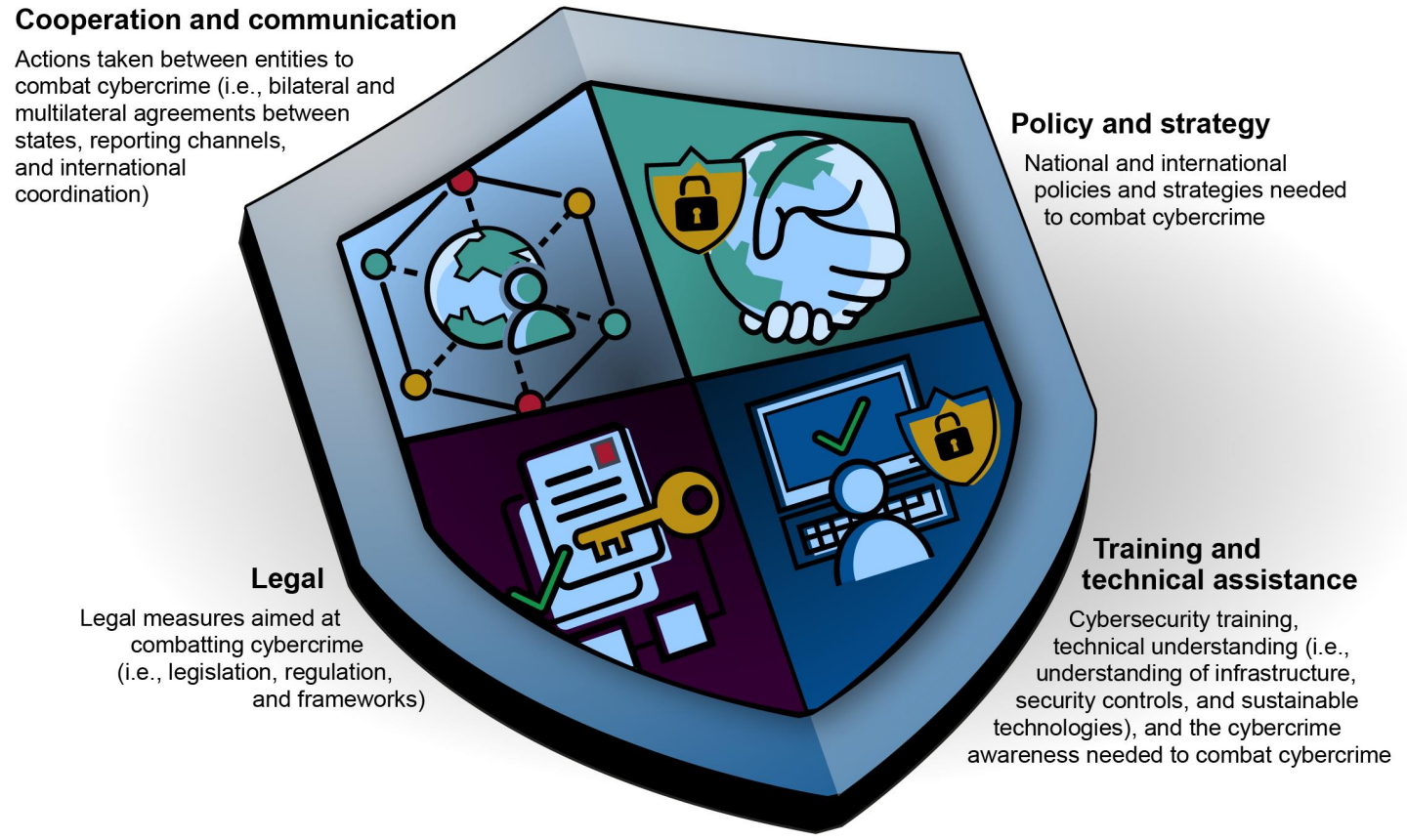
[10]In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime and responses to it by member states, the international community, and the private sector. This included the exchange of information on national legislation, best practices, technical assistance, international cooperation, and examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. The group released its draft comprehensive study on cybercrime in February 2013.

GAO Definition and Four Categories of Capacity Building to Combat Cybercrime

In order to collect and categorize U.S. efforts aimed at helping foreign nations combat cybercrime, we developed a definition of capacity building to combat cybercrime. For the purposes of this report, capacity building to combat cybercrime is defined as: assisting in enhancing nations' capabilities to combat cybercrime through the effective use of information and communications technologies and fostering responsible cybersecurity culture internationally.

Further, we identified four categories that capacity building activities can be grouped into, including encouraging cooperation and communication, creating legal measures, developing policies and strategies, and providing training and technical assistance. Figure 1 further describes our definitions for the four categories of capacity building to combat cybercrime.

Figure 1: Four Categories of Activities to Build Capacity to Combat Cybercrime



Source: GAO analysis; image: Buffaloboy/stock.adobe.com. | GAO-23-104768

Government-wide Plans and Strategies for Building Capacity to Combat Cybercrime

The federal government has developed plans and strategies that recognize the importance of addressing cybercrime and the ability to combat it on a global basis. For example, in 2019 the National Security Council expanded on the White House National Cyber Strategy's priority actions directing the U.S. government to build international cyber capacity. In 2022, the White House National Security Strategy prioritized promoting adherence to frameworks of responsible state behavior in cyberspace. The following table highlights additional plans and strategies for building capacity to combat cybercrime.

Table 1: Government-wide Plans and Strategies for Building Capacity to Combat Cybercrime

Plan or strategy	Roles and responsibilities
White House National Security Strategy (October 2022)	Assigns the Administration to: • Accelerate efforts to curb the threat posed by transnational organized crime by integrating law enforcement work with diplomatic, financial, intelligence, and other tools, in coordination with foreign partners • Deter cyberattacks from state and nonstate actors and respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure • Promote adherence to the United National General Assembly-endorsed framework of responsible state behavior in cyberspace
White House Fiscal Year 2020-2023 Joint Strategic Plan on Intellectual Property Enforcement (November 2020)	Directs the Department of Justice (DOJ) and State to continue to support deployment of a network focused on combatting the increasing ability and presence of transnational criminal organizations in intellectual property theft and on combatting cybercrime.
National Security Council National Cyber Strategy Implementation Plan[a] (June 2019)	Expands on the priority action from the National Cyber Strategy that directs the U.S. government to build international cyber capacity, including enhancing cyber capacity building efforts. Specifically, the plan directs State to: • Establish monthly interagency working group for cyber capacity building cooperation and coordination • Provide foreign assistance funding for cyber capacity to key allies and partners • Expand alignment of partners to U.S. cyber foreign policy and capacity building efforts
White House National Cyber Strategy of the United States of America (September 2018)	Directs the U.S. government to combat cybercrime and improve incident reporting. This includes: • Reduce threats from transnational criminal organizations in cyberspace • Improve apprehension of criminals located abroad through diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests • Strengthen partner nations' law enforcement capacities to combat criminal cyber activity, and develop solutions to potential barriers to gathering and sharing evidence • Urge effective use of existing international tools, and expand the international consensus favoring the Budapest Convention Directs the U.S. government to build international cyber capacity. This includes: • Enhance cyber capacity building efforts through expansion of automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges • Work to reduce the impact and influence of transnational cybercrime and terrorist activities by partnering with and strengthening the security and law enforcement capabilities of partners to build their cyber capacities
White House National Strategy to Secure Cyberspace (February 2003)	Designates the Department of Homeland Security as the lead agency to manage cyberspace incidents that could impact the nation. Designates DOJ as the lead agency to increase national efforts to investigate and prosecute cybercrime, including developing better data about victims of cybercrime in order to understand the scope of the problem and be able to track changes over time. Designates State as the lead agency to enhance international cyberspace security cooperation, including encouraging other nations to accede to the Budapest Convention.

Source: GAO. | GAO-23-104768

[a]The unclassified portion of the National Cyber Strategy Implementation Plan did not include certain priority actions from the National Cyber Strategy. Specifically, it did not include the strategy's priority actions directing the U.S. government to reduce threats from transnational criminal organizations in cyberspace, improve apprehension of criminals located abroad, and strengthen partner nations' law enforcement capacity to combat criminal cyber activity.

State, DOJ, and DHS Have Primary Responsibilities in Building Capacity to Combat Cybercrime

State, DOJ, and DHS have been assigned lead roles in building partner nations' capacity to combat cybercrime.[11] They are tasked with improving international law enforcement coordination in deterring and responding to cyber incidents, facilitating overseas investigations and prosecutions of cybercrime, and representing U.S. interests in international forums and treaties, among other things. Appendix II provides additional information on the agencies' priorities and goals, as documented in their strategic plans, and components' responsibilities and efforts to build international capacity to combat cybercrime.

State Promotes U.S Interests and Leads Foreign Assistance

State serves as the lead federal agency for foreign affairs and is responsible for the formulation, coordination, and oversight of foreign policy related to international communications and information policy. This includes exercising primary authority for the determination of U.S. positions and the conduct of U.S. participation in negotiations with foreign governments and international bodies. As part of those efforts, the department represents the U.S. in the Budapest Convention, and encourages other countries to join the treaty.

State's Joint Strategic Plan directs INL to apply foreign assistance to build partners' will and capacity to enhance the impact of U.S. enforcement and deterrence measures, and promote the adoption of international best practices in the form of legally binding treaties. In addition, INL's functional bureau strategy expands on the bureau's role to serve as the lead office for foreign assistance related to building capacity to combat

[11]We also interviewed officials from the Departments of Commerce, Defense, and the Treasury, and the Federal Communications Commission. However, we determined that State, DOJ, and DHS provide the majority of U.S. assistance in building international capacity to combat cybercrime.

cybercrime, including using appropriated funds to carry out these efforts.[12] Once INL receives funding, the bureau coordinates with other federal agencies to determine where the funds can be distributed by:

- conversing with implementers (e.g., DOJ's CRM and FBI, and DHS's ICE and Secret Service);
- assessing prioritization of activities and discussing where they rank during the time between soliciting ideas with implementers and receiving funding (e.g., fraudulent medicine was high priority during COVID-19);
- signing agreements (e.g., interagency agreement) between State and implementer once both parties agree on ranking of priorities and distribution of funds;[13] and
- beginning work outlined in agreement once the funds are available.

Additionally, INL sponsors, funds, and administers the International Law Enforcement Academy Program which aims to advance anti-crime efforts. To do so, the program focuses on building the capacity of the U.S. foreign criminal justice partners and connecting them to one another and to U.S. law enforcement to address shared threats. INL also funds the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN), which features the International Computer Hacking and

[12]State's functional bureau strategies articulate priorities within the department's functional areas and outline specific tradeoffs necessary to bring resources into alignment with department and U.S. Agency for International Development goals and objectives. Functional bureau strategies are also used to inform budget decisions, advise integrated country strategies, and shape performance reviews.

[13]An interagency agreement defines the financial details of an order, terms of reimbursement, itemized costs, and financial obligations when one agency performs services or provides items to another agency. All parties must agree to the interagency agreement terms and conditions, and an authorized official from each agency involved must sign it.

Intellectual Property (ICHIP) network.[14] INL co-manages GLEN with DOJ's Computer Crime and Intellectual Property Section and Office of Overseas Prosecutorial Development, Assistance, and Training.

- GLEN is a partnership between INL, the Computer Crime and Intellectual Property Section, and the Office of Overseas Prosecutorial Development, Assistance, and Training. It is a global law enforcement capacity building network of ICHIP attorney advisors, computer forensic analysts, and federal law enforcement agents. GLEN delivers training and technical assistance to foreign law enforcement and judicial partners to combat intellectual property and cybercrime activity; builds skills in the collection and use of electronic evidence to combat all types of crime, including transnational organized crime; and delivers targeted assistance to facilitate immediate help and encourage long-term institutional change.

Further, in April 2022, State established the Bureau of Cyberspace and Digital Policy. The bureau is intended to, among other things, lead diplomatic engagement on international cyberspace security in multilateral, regional, and bilateral forums and work with like-minded states to execute coordinated responses to malicious cyber activity.

DOJ Aims to Deter, Disrupt, Investigate, and Prosecute Cybercrime

DOJ, through CRM and the FBI, serves as the lead federal agency for cyber threat response and maintains primary domestic responsibility for investigating, disrupting, prosecuting, and deterring malicious cyber actors.[15] CRM has various sections executing its capacity building efforts through funding from State, including:

[14]The ICHIP network, a component of GLEN, is a program that deploys attorneys overseas to assess the capacity of law enforcement authorities, develop and deliver training, build and strengthen institutions, and monitor regional trends. DOJ funds one of the 12 ICHIPs: Bangkok, Thailand. State funds 11 of the 12 ICHIPs: Abuja, Nigeria; Addis Ababa, Ethiopia (African Union); Bucharest, Romania; European Crime Center at The Hague; Hong Kong SAR; Kuala Lumpur, Malaysia; Panama City, Panama; Sao Paulo, Brazil; Zagreb, Croatia; and two global ICHIPs located in Washington, D.C., Dark Web and Cryptocurrencies and Internet Fraud and Public Health. For example, the program's dark web and cryptocurrency ICHIP and internet-based fraud and public health ICHIP work through GLEN to support international capacity building aimed at countering cybercrime and intellectual property criminals, in the context of transnational organized crime.

[15]DOJ's National Security Division also investigates, prosecutes, and disrupts cybercrime. It focuses on criminals working for nation state actors, or whose crimes pose threats to U.S. national security.

- The International Criminal Investigative Training Assistance Program, which deploys active duty personnel and contract subject matter experts to conduct training and mentoring in investigations and develop the capacity of foreign counterpart agencies to carry out investigations.
- The Computer Crime and Intellectual Property Section, which prosecutes foreign nationals who commit electronic crime, provides international training on cybercrime, and participates in a number of international organizations addressing cybercrime.
- The Office of Overseas Prosecutorial Development, Assistance, and Training, which provides three main types of foreign assistance: (1) legislative assistance, including drafting and/or reviewing legislation to meet international standards; (2) skills capacity building, including skills development training and case-based mentoring; and (3) institutional building and reform, including assistance to help stand up and develop the skills of foreign country specialized cybercrime units.

The FBI's Cyber and Criminal Divisions also serve lead roles in investigating cybercrime. Among other things, the FBI's Cyber Division operates the National Cyber Investigative Joint Task Force in the Washington, D.C. region, which coordinates federal and international law enforcement and intelligence agencies' planning of multi-agency and multinational cyber disruption campaigns. Further, it works with international partners to investigate and attribute cybercrimes through experts deployed across more than 70 legal attaché offices worldwide. This includes almost 20 cyber assistant legal attachés trained and deployed to key international regions to focus exclusively on cyber matters.

DHS Works to Protect the U.S. against Cybercrime Threats

DHS serves as the lead federal agency for homeland security initiatives and takes actions to protect the American public from persistent cybercrime threats. DHS's strategic plan establishes Secret Service and ICE's Homeland Security Investigations as the department's operational components responsible for combatting cybercrime. The Secret Service safeguards financial infrastructure against computer fraud, cybercrime, and other electronic crimes. It works collaboratively with the FBI and other agencies at the National Cyber Investigative Joint Task Force to coordinate multi-jurisdictional and transnational cybercrime investigations. ICE's Homeland Security Investigations is assigned to:

- protect the U.S. against criminal organizations that threaten public safety and national security;
- combat transnational enterprises that seek to exploit American trade, travel, and financial systems;
- enforce criminal and civil federal laws; and
- provide training to foreign law enforcement agencies.

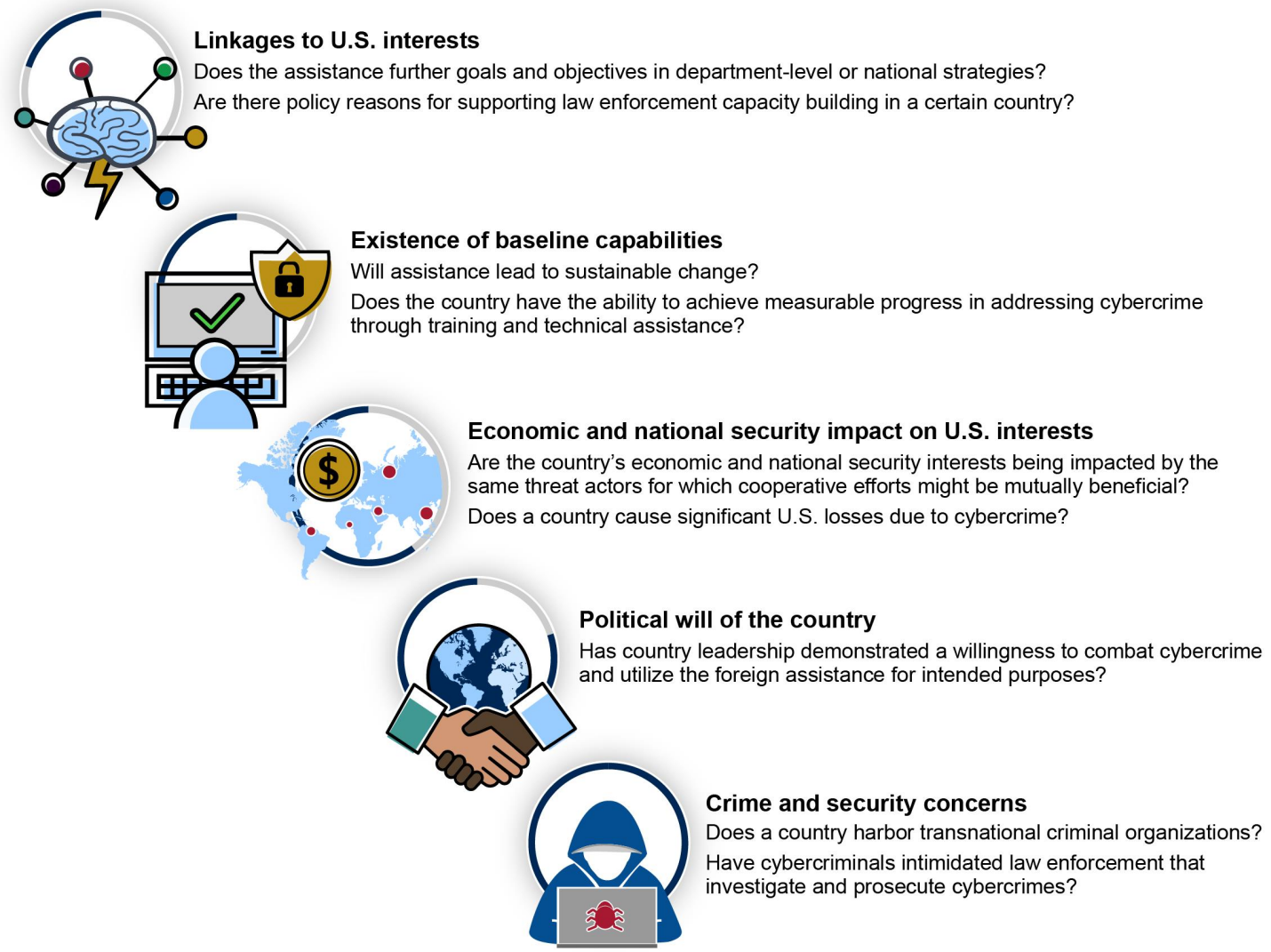
Further, in March 2022, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022.[16] The act, among other things, created within DHS's Cybersecurity and Infrastructure Security Agency, the Joint Ransomware Task Force. The task force is to convene interagency partners to coordinate an ongoing nationwide campaign against ransomware attacks.

State, DOJ, and DHS Consider Multiple Factors for Conducting Activities to Build Capacity to Combat Cybercrime

State's INL, DOJ's CRM and FBI, and DHS's ICE and Secret Service are to consider multiple factors when deciding which countries to assist. Specifically, the agencies are to determine (1) whether there are linkages to U.S. interests, (2) if baseline capabilities exist, (3) what the economic impact on U.S. interests will be, (4) what is the political will of the country, and (5) if there are crime or security concerns. Figure 2 presents the five key factors agencies are to consider.

[16]Division Y of the Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat. 49, 1038 (2022).

Figure 2: Key Factors Agencies Are to Consider When Providing Assistance to Build Capacity to Combat Cybercrime



Source: GAO; images: Buffaloboy/stock.adobe.com, | GAO-23-104768

Agencies' component entities also highlighted a few factors that contribute to their decision making processes. Specifically:

- INL is to consider where the highest level of cybercrime engagement is most likely to lead to sustainable change that matters to U.S. policy and priorities. It then is to affirm that the overall goals and objectives of its capacity building activities are closely linked to its cybercrime strategic guidance, functional bureau strategy, department strategic

plan, integrated country strategies, and intellectual property rights agreement with DOJ's Office of Overseas Prosecutorial Development, Assistance, and Training.

- CRM is to provide foreign assistance based on requests from either the country itself or the U.S. embassy in that country. CRM is to coordinate with the embassy, which often has a cyber working group and a DOJ official at that post. CRM also is to coordinate with appropriate functional and regional bureaus at State to tailor its assistance efforts.
- The FBI is to identify countries that contain a nexus to the cyber threats affecting the U.S. for which the agency has prioritized its investigative and intelligence efforts.
- ICE foreign field office officials are to communicate the needs of the country to program officials. Based on their availability, officials are to provide training to increase local law enforcement's capacity to combat cybercrime and thus assist ICE in future investigations.

GAO Has Previously Reported on Challenges in Tracking and Combatting Cybercrime

We have been reporting on the federal government's challenges in tracking and combatting cybercrime since 2007. For example:

- In 2007, we reported that numerous public and private entities faced challenges in protecting against, detecting, investigating, and prosecuting cybercrimes.[17] These challenges included limitations in reporting cybercrime, ensuring adequate law enforcement analytical and technical capabilities, working in a borderless environment with laws of multiple jurisdictions, and implementing information security practices and raising awareness.
- In 2010, we reported that federal agencies, including DHS, DOJ, and State, had responsibilities for international cyberspace governance and security efforts and were involved in efforts to develop international standards, formulate cyber defense policy, facilitate overseas investigations and law enforcement, and represent U.S. interest in international forums.[18] We noted that agencies faced

[17]GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,* GAO-07-705 (Washington, D.C.: June 22, 2007).

[18]GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO-10-606 (Washington, D.C.: July 2, 2010).

challenges in developing a comprehensive national strategy that specifies overarching goals and outcome-oriented performance metrics; participating in international cyber-incident response; investigating and prosecuting transnational cybercrime amid a plurality of laws, varying technical capabilities, and differing priorities; and providing models of behavior that shape policies and activities of countries. Further, we noted that the U.S. had been unable to define cyberspace-related norms that may be necessary for guiding U.S. responses to cyber incidents.

We made five recommendations aimed at addressing challenges the U.S. faces in addressing global cybersecurity and governance, four of which were implemented. The recommendation that was not implemented was that the White House, in collaboration with State, DOJ, and DHS, among others, develop a comprehensive national global cyberspace strategy that (1) articulates overarching goals, subordinate objectives, specific activities, performance metrics, and reasonable time frames to achieve results; (2) addresses technical standards and policies while taking into consideration U.S. trade; and (3) identifies methods for addressing the enforcement of U.S. civil and criminal law. Though an international strategy for cyberspace was published in May 2011 and included some key characteristics, it did not establish specific activities, performance metrics, or time frames for achieving results.

Challenges in Building Global Capacity to Combat Cybercrime

The U.S. government faces challenges in trying to build foreign nations' capacity to combat cybercrime, similar to challenges it faces in implementing foreign assistance. Among the challenges that State's INL, DOJ's CRM and FBI, and DHS's ICE and Secret Service identified were the availability of experts to provide assistance, the rapidly evolving advancements in technology, and a general lack of agreement on what constitutes a "cybercrime." Additionally, we conducted an expert panel with seven members from international entities who also identified challenges in building partner nations' capacity to combat cybercrime as well as challenges they face in working with the U.S. government on these efforts. Appendix III provides additional information on the expert panel.

Federal Officials and International Experts Identified Six Challenges to Building Capacity to Combat Cybercrime

Officials from State, DOJ, and DHS, as well as experts from international entities, identified several challenges related to assisting foreign nations in building their capacity to combat cybercrime. The most commonly identified challenges were the lack of available resources and difficulty in retaining trained individuals. Other challenges included the rapidly evolving technological landscape and inconsistent definitions of "cybercrime."

- **Foreign nations' lack of dedicated resources (e.g., qualified personnel, technology, and funding).** State, DOJ, and DHS officials all presented this challenge. State officials explained that developing nations tend to have fewer resources, which in turn can make it more difficult to effectively receive cybercrime training. A DOJ official also stated that the inconsistent nature in which resources are dedicated to combatting cybercrime on the recipient country's side is a constant challenge. One international expert noted that developing countries may not see cybercrime as a significant issue, and thus they do not devote resources, time, or effort. Another expert noted that they conducted training for law enforcement officers without computers or a digital forensics lab with internet access.
- **Difficulties in retaining highly trained staff.** State and DOJ officials noted that trained individuals become valuable and often move to the private sector for higher positions or pay. As such, foreign partners are constantly losing trained individuals, which creates a need for continuous training to address the resulting knowledge gap. Similarly, two international experts stated that trained individuals become valuable and may be promoted or move to a different section of law enforcement, and do not pass down the training to their replacements. They highlighted that there is also a lack of career paths enticing trained individuals to stay in their organizations, utilize those skills, and mentor others.
- **Foreign nations' limited ability to effectively implement the training provided.** DHS officials stated that when providing foreign assistance, local governments often face challenges with identifying and finding the appropriate people to understand and effectively use the assistance they are receiving. A DOJ official noted that sometimes senior level officials do not allow line level officials to implement new best practices, such as tools or techniques, learned through U.S. government assistance. Thus, the U.S. government often conducts training for the senior level officials before delivering it to the

employees directly engaged in the work. Similarly, an international expert noted that individuals may receive training due to their political influence, rather than because they are involved in this arena.

- **U.S. government's capacity to provide assistance.** State officials commented that the federal government's own capacity, such as availability of experts, to deliver assistance to foreign partners and international law enforcement is a challenge. An international expert noted that, compared to other areas, U.S. funds devoted to capacity building to combat cybercrime remain relatively small, and sometimes demand for equipment (e.g., computers and servers) exceeds supply.

Government officials, international entities, and private sector organizations often have their own definitions of cybercrime, such as:

- DOJ generally categorizes cybercrime as those offenses in which a computer or data is the target of the criminal activity, such as network attacks and intrusions. DOJ also recognizes that cyber-enabled crimes, which are offenses in which a computer facilitates the scale, scope, or speed of a crime in a way that would not be feasible without use of a computer, may fall within a more broad categorization of cybercrime.
- State focuses its efforts to address cybercrime on instances where computer systems, networks, and data are targeted or misused.
- The Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030) is an important law to address cybercrime. It generally classifies seven types of activities that are punishable as crimes when affecting protected computers, including knowingly transmitting a program, code, or command that intentionally causes damage to a protected computer; or, with the intent to extort something of value, transmitting in interstate or foreign commerce any communication containing a threat to cause damage to a protected computer.[a]
- The Budapest Convention categorizes cybercrime as offenses against and by means of computer systems.
- The United Nations Office on Drugs and Crime defines cybercrime as an act that violates the law, which is perpetrated using information and communications technologies, to either target networks,

systems, data, websites, and/or technology or facilitate a crime.

Source: GAO analysis of entities' reports. | GAO-23-104768

[a]The seven criminal activities are established in 18 U.S.C. § 1030(a)(1)-(7). The term "protected computer" has an expansive definition that includes a computer used by or for the federal government or a financial institution and the use is impacted by the criminal activity, or a computer that is used in or affecting interstate or foreign commerce or communication.

- **Rapidly evolving technologies used in cybercrime.** State officials stated that the constant advances and the spread of technology expands the field of play for criminals. Similarly, an international expert noted that individuals need continuous updates on trainings in order to keep up with the pace of evolving technology.
- **Inconsistent definitions of "cybercrime."** Both agency officials and international experts noted that the lack of an agreed upon definition for what constitutes cybercrime, within governments and globally, presents a barrier to tracking data on the current scope and prevalence of cybercrime. DOJ officials stated that some countries consider all computer-facilitated crimes to be cybercrimes, whereas other countries' cybercrime units focus on investigations involving digital evidence and forensic examinations. DHS officials noted that inconsistencies in defining cybercrime leads to varying reporting and tracking requirements, and thus makes the true cost and impact difficult to measure. An international expert also noted that different interpretations of cybercrime can make it difficult to measure the cost and impact it creates, and thus convey the significance of cybercrime.

International Experts Identified Challenges in Working with the U.S. Government

Regarding panelists' comments on difficulty obtaining information:

A DOJ official agreed that there is not significant transparency on funding. The official noted that the agency is aware of money that it will receive for capacity building activities, but does not have insight into the total amount of funding that State receives to carry out its overall capacity building activities.

Some DHS officials agreed that most international law enforcement entities are

unaware on how to request funding information. These international law enforcement entities rely on State's field point of contact to navigate the various layers of formal requests.

Some DHS officials disagreed and noted that not all assistance should be done with public announcement. Specifically, for direct assistance, one official said it is more appropriate to directly engage with the relevant foreign partner rather than to publicly announce the process (e.g., providing technical assistance or case-based mentoring on a criminal investigation with foreign law enforcement should not be publicly announced).

Source: GAO analysis of agency documentation. | GAO-23-104768

Our expert panel representing seven international entities identified challenges they face when coordinating with the U.S. government in assisting foreign nations and international criminal justice entities in building their capacities to combat cybercrime. These challenges included difficulty obtaining information, lack of communication, limitations regarding the use of funds, and difficulty disseminating classified intelligence. We also presented the challenges that the experts highlighted in working with the U.S. to State, DOJ, and DHS officials. We provided the officials the opportunity to comment on the challenges, with their responses included in the sidebars. The challenges the experts presented include the following:

- **Difficulty obtaining information.** Aiding partners, such as the international entities engaging and working with U.S. embassies, find it difficult to get information on activities from U.S. agencies and embassies because activities are funded through different sources.
    - International experts stated there is a lack of transparency with funding and funding information is not summarized anywhere and is not available for partners to review.
    - Panelists also noted a fragmentation of funding sources; specifically, partners must go through multiple different sources to obtain funding information (i.e., partners may need to check four different sources directly to obtain funding information).

Regarding panelists' comments on lack of collaboration:

Some DOJ officials disagreed and noted the following:

- Coordination is a challenge for every donor country, including multilateral donors (e.g., Council of Europe and United Nations), not just the U.S. The U.S. government has working groups within each U.S. embassy that help organize meetings to ensure appropriate issues are being addressed and that there is coordination among U.S. assistance providers.
- Assistance efforts are typically coordinated with other members of the country team who have a role or need to know. For broader capacity building efforts, a legal attaché office often provides awareness and coordination through the post's cyber working group.

- **Lack of collaboration.** Aiding partners experience collaboration issues and do not receive information in advance from the U.S. government.
  - According to the panel, it is difficult to understand the full scope of the U.S. government's efforts because activities are executed by components and not included in a wider program.
  - Aiding partners do not know in advance what is going on or if there is a plan (e.g., week-long trainings on a yearly basis or eight stages and modules for trainings).
  - International experts stated it is difficult to keep in constant contact and coordinate efforts because there are many players in this field.
- **Lack of dedicated funding streams.** U.S. government money that is allocated to capacity building is discretionary and there are not often dedicated funding streams.
  - According to the panel, allocated funds depend on the priorities of the officials in charge of the bureau providing funds.
- **Limitations regarding the use of funds.** Aiding partners face limitations on where and for what purposes funds can be used (e.g., certain countries the U.S. cannot fund activities in).
  - International experts stated that obtaining funds for programs that include various activities can be difficult because there are restrictions on how funds can be used (e.g., funds allocated to State need to fall under certain criteria).
  - According to the panel, countries that harbor cybercriminals are prime spots for ransomware and could benefit from receiving assistance, but the U.S. government does not typically offer assistance in those countries.

A DHS official disagreed and noted that perfect coordination is not achievable and should not be pursued at the expense of agile execution that can efficiently achieve the objectives of U.S. national strategies. The country team is generally the best situated to resolve such issues mentioned.

Source: GAO analysis of agency documentation. | GAO-23-104768

Regarding panelists' comments on lack of dedicated funding streams:

Some DOJ officials agreed and stated that they are not aware of any strategic document from State which outlines the recipients or the particular activities for which the funds are to

Regarding panelists' comments on limitations regarding the use of funds:

Regarding limitations on funds, U.S. officials neither agreed nor disagreed and noted the following:

- Some DOJ officials said they do not receive appropriations available for capacity building the way that State does, and thus any activities they conduct with funds from State are subject to the requirements and authority of the Foreign Assistance Act.
- Some DHS officials noted that the Foreign Assistance Act is the primary law authorizing these forms of assistance and it has restrictions that limit how such funds can be used. However, further consideration of how to

Regarding panelists' comments on confusion in vetting process:

Some DOJ officials neither agreed nor disagreed and noted that all implementing agencies using foreign assistance funds from State are required to follow the Leahy vetting requirements.

Some DHS officials agreed that Leahy vetting could increase the administrative cost and constrain the scheduling of assistance activities.

Source: GAO analysis of agency documentation. | GAO-23-104768

Regarding panelists' comments regarding difficulty disseminating classified intelligence:

Some DOJ officials disagreed and noted that they are unaware of any other national government downgrading or declassifying more intelligence than the U.S. for such purposes, particularly public attributions of malicious cyber activity. The U.S. government has been making cyber threat reporting increasingly available to partner countries, targeted private sector entities, and the general public, but highly compartmented single source information can be difficult to process and share.

Source: GAO analysis of agency documentation. | GAO-23-104768

- **Confusion in vetting process.** According to the panel, vetting countries against the "Leahy law" adds additional work for international participants.[19] In addition, some participants do not understand the process and it can be more difficult for participants that do not have contacts at U.S. embassies.
- **Difficulty disseminating classified intelligence.** International experts stated that the U.S. government has found it more difficult than others to convert highly classified intelligence to a level that is needed for public awareness.
    - Difficult to receive a single unified view from the U.S. government on a particular topic due to national security and intelligence sharing challenges.

Agencies Conducted Activities to Build Capacity to Combat Cybercrime but Have Not Comprehensively Evaluated Collective Efforts

State's INL, DOJ's CRM and FBI, and DHS's ICE and Secret Service have conducted a variety of activities related to encouraging cooperation and communication, creating legal measures, developing policies and strategies, and providing training and technical assistance in an effort to build foreign nations' capacity to combat cybercrime. In addition, these agencies have documented case-specific accomplishments for many activities. However, State, which is in the best position to conduct a comprehensive evaluation of the agencies' collective efforts, has not yet done so. Thus, the ability to demonstrate long-term successes or institutional change due to State's investments remains unclear.

[19]The "Leahy law," informally named after Senator Patrick Leahy, who sponsored the bill that was enacted, consists of two statutory provisions that prohibit U.S. assistance to a foreign security force unit when there is credible information that the unit has committed a "gross violation of human rights." State's Leahy law is applicable to assistance authorized by the Foreign Assistance Act of 1961, as amended, or the Arms Export Control Act, as amended, and is codified at 22 U.S.C. § 2378d. A similar provision applicable to funds made available to the Department of Defense is codified at 10 U.S.C. § 362.

State, DOJ, and DHS Executed Various Efforts to Build Capacity to Combat Cybercrime

Encouraging International Cooperation and Communication

State, DOJ, and DHS conduct activities to combat cybercrime to assist in fostering responsible cybersecurity culture and enhancing international cooperation. The following table provides examples of actions that agencies have taken towards cooperation and communication.

Table 2: Examples of Agencies' Efforts to Encourage International Cooperation and Communication

Department	Agency	Overall efforts	Reported case-specific examples
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Shares ideas with foreign nations on ways to better cooperate in identifying, prosecuting, and punishing cyber and intellectual property criminals.	Assisted in establishing new working groups in Southeast Europe and Southeast Asia, specifically by the International Computer Hacking and Intellectual Property networks in Zagreb, Croatia, and Kuala Lumpur, Malaysia, to enable foreign law enforcement partners to better coordinate and share information to combat the criminal misuse of virtual currencies.
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Encourages bilateral relationships with countries worldwide, as well as multilateral relations with the Group of Seven,[a] United Nations, Organization of American States, African Union, and Association of Southeast Asian Nations, to promote American policies on cybercrime and intellectual property crime enforcement.	Deployed an International Computer Hacking and Intellectual Property attorney to the African Union in Addis Ababa, one of the network's locations overseas, to strengthen cooperation and coordination assistance in Sub-Saharan Africa.
Department of Justice	Criminal Division	Works with international entities, such as the European Commission, the Group of Seven, the Group of 20,[b] and United Nations, to improve international cooperation and coordination to combat online child sexual exploitation.	Helped negotiate a resolution addressing crimes against children, which was adopted by the United Nations General Assembly in 2019.
Department of Homeland Security	U.S. Secret Service	Engages in information sharing with foreign partners, in coordination with State through the International Law Enforcement Academy Program, concerning cyber-enabled crimes in order to build mutual resilience across global ecosystems that are subject to illicit financial attacks.	Collaborated with participants from International Law Enforcement Academies courses conducted in the Caribbean, Thailand, Botswana, Nigeria, and South Africa, for example, to leverage their intelligence and pre-established source relationships on U.S. veiled exchanges in their regions.

Source: GAO analysis of agency documentation. | GAO-23-104768

[a]The Group of Seven is an intergovernmental forum consisting of the U.S., Canada, France, Germany, Italy, Japan, and the United Kingdom. The Group of Seven develops initiatives to address global security and economic crises, prioritizes cybersecurity, and operates the Group of Seven 24/7 Cybercrime Network.

[b]The Group of 20 is an intergovernmental forum comprising of 19 countries and the European Union, and works to ensure secure and resilient digital economy and encourage cross border cooperation.

Creating Legal Measures

State and DOJ collaborate with international entities to draft legislation that aligns with international treaties for combatting global cybercrime. Table 3 provides examples of these efforts to create legal measures.

Table 3: Examples of Agencies' Efforts to Create Legal Measures

Department	Agency	Overall efforts	Reported case-specific examples
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Provides legislative drafting assistance to legislators in countries establishing legal frameworks related to cybercrime and intellectual property protection.	Delivered legislative drafting advice to Brazil, Tonga, and Nigeria on how to strengthen their laws to conform with the Budapest Convention, through the Global Law Enforcement Network.
Department of Justice	Criminal Division	Delivers legislative review, commentary, and drafting assistance to ensure countries' legislation is in line with the Budapest Convention.	Led engagement, through its Maldives cybercrime working group in coordination with the Maldives Police Service and guidance by the Council of Europe and its legislative experts, on drafting new cybercrime legislation and the amendment of the criminal code to meet international standards, specifically those in the Budapest Convention.

Source: GAO analysis of agency documentation. | GAO-23-104768

Developing Policies and Strategies

State and DOJ collaborate with countries to develop policies and strategies to sustain progress in combatting cybercrime. Table 4 lists examples of how DOJ and State have assisted in developing policies and strategies.

Table 4: Examples of Agencies' Efforts to Develop Policies and Strategies

Department	Agency	Overall efforts	Reported case-specific examples
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Provides assistance to foreign partners to align their policies with global best practices and existing international agreements, and strengthens partners understanding of good cybersecurity policy and best practices to address cybercrime.	Provided the government of Ghana, in coordination with State's Bureau of African Affairs and private sector partners, with feedback on its national cybersecurity policy and strategy. This feedback included input on cybercrime elements, in order to help shape Ghana's implementation of its strategy as well as national legislation covering this topic.

Department	Agency	Overall efforts	Reported case-specific examples
Department of Justice	Criminal Division	Offers support to foreign partners to update national strategies and policies.	Conducted week-long symposia for judges, prosecutors, and law enforcement officials from 30 different countries in Africa, Central America, the Caribbean, and the Balkans. The symposia focused on building a comprehensive national response in each country for combatting various types of cybercrimes, including policy and enforcement guidance.

Source: GAO analysis of agency documentation. | GAO-23-104768

Providing Training and Technical Assistance

State, DOJ, and DHS provide training and technical assistance to combat cybercrime. Table 5 provides examples of the training and technical assistance.

Table 5: Examples of Agencies' Efforts to Provide Training and Technical Assistance

Department	Agency	Overall efforts	Reported case-specific examples
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Funds bilateral and multilateral cybercrime and intellectual property theft training and technical assistance to strengthen foreign partner enforcement capacity, particularly through its Global Law Enforcement Network.	Offered regional workshops to foreign law enforcement partners through the Global Law Enforcement Network. Topics included the handling of electronic evidence, virtual currencies, the dark web, and ransomware attacks on public health institutions.
Department of Justice	Criminal Division	Leverages foreign assistance funding to provide training and technical assistance, including cybercrime forensic lab and training center equipment.	Provided technical assistance, training, and equipment to Nepal Police and Armed Police Force in order to develop new provincial police organizations. The training was focused on police leadership, improved culture and education, and increased police capabilities to investigate cybercriminals.

Department	Agency	Overall efforts	Reported case-specific examples
Department of Justice	Federal Bureau of Investigation	Provides training to foreign law enforcement officers that focuses on the history and interworking of the internet and tools and techniques to assist in their investigations.	Delivered intermediate and advanced cyber courses in Hungary through the International Law Enforcement Academies and its legal attachés. The course provided law enforcement officers a more in-depth understanding of the internet, tools, and techniques to assist in investigations, and pathways to share intelligence and information. Hosted, on an annual basis, cyber law enforcement and analytic counterparts at the National Cyber Forensics and Training Alliance International Exchange Program. The program focused on embedding cyber personnel from other countries with the Federal Bureau of Investigation and industry partners for several weeks in a field office environment. Participants shared best practices, networked with one another, and jointly investigated international cybercrime cases. The program encouraged on the job training and real world results that international partners could continue to pursue in their home countries.
Department of Justice	Federal Bureau of Investigation	Provides technical assistance to foreign nations through directly embedding with foreign law enforcement partners on a long-term basis and ad hoc deployment to foreign nations requesting assistance in response to a specific cyber incident.	Trained and deployed numerous cyber assistant legal attachés to embed with embassies and work directly and daily with international law enforcement on cybercrime investigations. These relationships have enhanced the speed and reliability of information sharing, and joint investigations and operations planning between the bureau and its foreign partners. Developed 24/7 on-call cyber incident response specialists, through its cyber action team, who deploy to significant cyber incidents. The cyber action team deployed and facilitated the U.S. government's response and assistance to cyberattacks on and threats to Albania, Montenegro, Qatar, and Ukraine.

Department	Agency	Overall efforts	Reported case-specific examples
Department of Homeland Security	U.S. Immigration and Customs Enforcement	Delivers investigative assistance, cyber training, and equipment to support international law enforcement and investigations of cyber-related crimes.	Conducted various cybercrime courses such as: • Countering online child abuse workshop in Ghana, Sierra Leone, Gambia, and Liberia in coordination with Senegal and the United Nations Office on Drugs and Crime; • Online investigations workshops in South Africa, Moldova, Cyprus, the United Arab Emirates, Malaysia, and India, in coordination with State, for police officers; • Dark web/cryptocurrency investigation courses in Portugal and Spain for police officers; and • Digital forensic first responder session in Serbia, in coordination with DOJ, for Serbian law enforcement officers.
Department of Homeland Security	U.S. Secret Service	Provides various courses to international partners to assist in combatting the transnational threat, such as basic investigations of computers and electronic crimes program, cybercrime tactical courses, investigating criminal use of cryptocurrency, and women in law enforcement leadership course.	Led training for Caribbean partners through the International Law Enforcement Academies executive courses. The training consisted of the review, analysis, and action of standing laws and regulations in banking systems and illicit movement channels exploited by criminals.

Source: GAO analysis of agency documentation. | GAO-23-104768

Agencies Have Measured Outcomes of Capacity Building Activities, but State Has Not Conducted a Comprehensive Evaluation

According to the GPRA Modernization Act of 2010, agency performance plans should, among other things, establish performance goals, describe how those goals contribute to the goals and objectives established in the agency's strategic plan, and provide a description of how performance goals are to be achieved.[20] Further, the act requires agencies to establish a set of performance indicators to be used in monitoring progress toward each performance goal, including output and outcome indicators. Additionally, agencies should submit updates on agency performance that

[20]The GPRA Modernization Act of 2010, Pub. L. No 111–352, § 3, 124 Stat. 3866, 3867 (2011) revised requirements established by the Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285 (1993), and added new performance-related requirements.

compare actual performance achieved with the performance goals established in the agency performance plan.

State's, DOJ's, and DHS's strategic plans included goals, described how the goals contributed to departmental priorities and objectives, and established how the goals were to be achieved (see appendix II). In addition, the three agencies used various means to measure outcomes of their activities to build capacity to combat cybercrime. For example, State, DOJ, and DHS:

- conducted surveys after providing training and asked trainees if the course content was delivered in a timely and efficient manner and if it would be used in their daily practice;
- engaged with law enforcement to determine if arrests, convictions, or extraditions of personnel engaged in crimes have been made using knowledge and skills acquired via U.S. government assistance;
- assessed the number of fulfilled requests for training courses;
- considered the number of countries that request accession to the Budapest Convention; and
- determined if communication channels between international partners have been established.

Additionally, the three agencies provided reported outcome measures and case-specific accomplishments (see table 6).

Table 6: Examples of Agencies' Reported Outcome Measures and Case-specific Accomplishments

Department	Agency	Reported outcome measures	Reported case-specific accomplishments
Department of State	Bureau of International Narcotics and Law Enforcement Affairs	Instances of: • participants using the skills they learned in daily practice, or initiating subsequent successful investigations or prosecutions; • partnering nations' willingness to engage in timely and responsive information sharing in regional or international settings; • requests for additional training and other resources; • assessments and reports completed by the Global Law Enforcement Network; and • number of countries that request accession to the Budapest Convention.	• Romanian government expanded one of its training programs, with support from State, and established the National Cyber Security Directorate and an institutional cyber working group, both meant to build Romania's ability to combat cybercrime. • The government of Ghana updated national legislation and national cybersecurity policy and strategy, which included cybercrime elements, and thus was able to become a member of the Budapest Convention. As a result of cyber training courses: • Philippines National Police and Filipino Anti-Cybercrime Group were instrumental in identifying and neutralizing threats, including passing along intelligence and arresting a suspect after monitoring terrorist groups' social media feeds. • Colombian investigators assisted in capturing members of a terrorist group by extracting evidence from recovered laptops. • Kosovo police recovered numerous technological artifacts from terrorist groups that contained propaganda videos, among other things. • Bosnia and Herzegovina's State Investigation and Protection Agency and local police arrested terrorist suspects and seized weapons and explosives.
Department of Justice	Criminal Division	Institutional development, such as: • setting up a specialized unit that focuses on building capacity to combat cybercrime; • new partnerships established between foreign countries; • foreign nations enact legislation that aligns with the Budapest Convention; and • new standard operating procedures that better address cyber issues.	• Indonesian police assisted in major terrorism investigations due to the cybercrime unit, cybercrime forensic laboratory, and training center that Criminal Division officials helped them develop. • Ukraine's Ministry of Internal Affairs Forensic Center, with support from Criminal Division officials, seized over 50 servers and computers from a Ukrainian internet service provider as a result of a child pornography investigation. This also led to the arrest of over 150 people in the U.S. and other countries, and uncovered connections in more than 30 countries tied to a global child pornography ring.

Department	Agency	Reported outcome measures	Reported case-specific accomplishments
Department of Justice	Federal Bureau of Investigation	Instances of: • Legal attaché's enhanced relationships with their partners (i.e., foreign law enforcement and intelligence agencies), that lead to greater speed and reliability of information sharing and joint investigation and operations planning; • contributions to the advancement of bureau investigations; • case-specific accomplishments (i.e., requests fulfilled, actions taken, arrests of current cyber cases or fugitives, and judicial outcomes); and • retention of trained individuals.	• Kazakhstan participants provided positive verbal feedback on a cyber training course provided by the Federal Bureau of Investigation, and noted the country planned to incorporate the training as a step for additional and more advanced cyber courses. • German law enforcement officers and the Federal Bureau of Investigation seized a dark web market place, and with the seized materials were able to identify and target vendors selling narcotics and weapons. In coordination with Europol, officials facilitated independent but collaborative global investigations and enforcement operations that resulted in over 100 arrests, over 200 kilograms of drugs seized, and over $30 million in cash and cryptocurrency seizures.
Department of Homeland Security	U.S. Immigration and Customs Enforcement	Increase in requests from foreign partners for ongoing engagement, cyber capacity building training, and positive feedback from partners on previous engagements.	• Received positive feedback through course evaluations for trainings conducted in various countries, such as Serbia, the United Arab Emirates, and Vietnam. Participants reported more knowledge of computer forensics tools and software, illicit activity facilitated via the dark web, and internet investigative techniques, among other things, and expressed interest in more advanced training for analyzing and reporting data.
Department of Homeland Security	U.S. Secret Service	Effective cooperation and multijurisdictional intelligence sharing from foreign law enforcement partners.	• Caribbean partners assisted in the location, surveillance, and arrest of a high-profile target responsible for multijurisdictional victim fraud schemes. • Bangkok partners played a key role in the recovery of millions of dollars associated with an account takeover scheme that victimized a U.S. citizen. • Nigerian participants, from International Law Enforcement Academies courses in Botswana, contributed to intelligence sharing on unknown banking pathways. This helped in identifying assets associated with a major third party money laundering target responsible for U.S. victim fraud.

Source: GAO analysis of agency documentation. | GAO-23-104768

State Has Not Conducted a Comprehensive Evaluation of Collective Efforts

In addition to federal requirements for agency performance, State has its own requirements for program performance and evaluations.[21] Specifically, State's policy calls for one evaluation of every major program once in its lifecycle or once every 5 years.[22] Thus, INL is required to conduct a program evaluation for its capacity building activities and those that it funds. In contrast to performance monitoring, program evaluations typically examine a broader range of information on program performance and its context than is feasible to monitor on an ongoing basis.[23] Further, *Standards for Internal Control in the Federal Government* state that management should design control activities to achieve objectives and respond to risks, and establish and operate monitoring activities to monitor the internal control system and evaluate the results.[24]

State has controls in place to assess whether aspects of its programmatic efforts for building global capacity to combat cybercrime are achieved. For example, INL's working evaluation plan for fiscal year 2022 includes an evaluation of a regional forensics training center in Estonia. Part of the evaluation is intended to include determining if the country is compliant with international standards and if target goals were met. If target goals were not met, State would determine the cause such as a lack of training or mentorship. Officials noted that choosing one project of a major program to evaluate, such as the Estonia project, would fulfill the

[21]Department of State, *Foreign Affairs Manual*, 18 FAM 301.4 (2018).

[22]In 2021, State changed its requirements for program evaluations. The new requirements call for one evaluation of every major program once in its lifecycle or once every 5 years. INL defines its major programs as each objective of the functional bureau strategy. INL's capacity building activities are linked to an objective in its functional bureau strategy, specifically that international partners have greater ability to counter cybercrime. Thus, the activities are subject to the department's major program evaluation requirements.

[23]For further information about program evaluation and the distinction between performance monitoring and program evaluation, see GAO, *Program Evaluation: Key Terms and Concepts,* GAO-21-404SP (Washington, D.C.: Mar. 22, 2021); and *Performance Measurement and Evaluation: Definitions and Relationships (Supersedes* GAO-05-739SP*),* GAO-11-646SP (Washington, D.C.: May 2, 2011).

[24]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

department's evaluation requirements.[25] Further, officials stated that they are not required to conduct a comprehensive evaluation of programs for building global capacity to combat cybercrime and thus have not done so.

However, State receives appropriated funds from Congress available for building global capacity to combat cybercrime. Additionally, State is authorized to provide funding to DOJ and DHS in order for them to execute activities to build global capacity. Although the Estonia evaluation may meet the department's evaluation requirements, it is not a comprehensive evaluation of collective efforts which ensures programs are achieving intended goals rather than just individual projects. Further, Estonia has a robust technical infrastructure compared to other nations who may receive funds from State to support capacity building. Specifically, according to the International Telecommunication Union *2020 Global Cybersecurity Index,* Estonia ranked third of the 194 participating countries.[26] As such, these international partners might not be as equipped as Estonia to provide State the level of data required to conduct a comprehensive evaluation of the totality of the department's efforts. A comprehensive evaluation could better position State to ensure that its capacity building efforts and those that it funds are meeting department and whole-of-government objectives: to strengthen partner nations' law enforcement capacity to combat transnational criminal activity and to enhance international cyber capacity building efforts.

Until State conducts a comprehensive evaluation of the program for building global capacity to combat cybercrime, Congress may lack key information needed to determine whether program objectives are being met and contributing to long-term success in improving foreign nations' ability to more effectively combat cybercrime. Additionally, without a comprehensive evaluation, State may lack key information needed to make fully informed decisions when providing funding to DOJ and DHS

[25]INL's Implementation Guidance for the Department's Evaluation Policy states that evaluating a subset of the program is acceptable provided the evaluation addresses critical questions related to the program or project's intended outcomes. Thus, one office's decision to evaluate an intervention under a particular functional bureau strategy objective can satisfy the bureau-level requirement to evaluate that objective. However, INL's evaluation guidance also notes that these evaluation requirements are minimum requirements and allow for more frequent evaluations to meet learning and accountability needs.

[26]International Telecommunication Union, *Global Cybersecurity Index 2020* (Geneva, Switzerland: 2021). The Global Cybersecurity Index measures countries' commitment to cybersecurity. The index maps 82 questions on the 194 participating countries' cybersecurity commitments across five pillars: legal measures, technical measures, organizational measures, capacity development measures, and cooperation measures.

for capacity building purposes. Further, the U.S. will have a limited understanding of its overall effectiveness in aiding international partners in their ability to fight cybercrime.

Conclusions

Cybercrime incidents continue to grow in frequency and scale across numerous countries and legal jurisdictions. Thus, U.S. efforts to build foreign nations' capacity to combat cybercrime are critical to the economic and national security of the U.S. and its global partners. Accordingly, State, DOJ, and DHS have conducted numerous activities to build foreign nations' capacity to combat cybercrime, including encouraging cooperation and communication and providing training and technical assistance.

In addition, State, DOJ, and DHS have established goals for efforts to build capacity to combat cybercrime and have reported case-specific accomplishments. However, in its leading role for foreign assistance, State has not conducted a comprehensive evaluation of how these activities have contributed to overall capacity building. Without such evaluations, State cannot ensure that agencies' individual activities or case-specific accomplishments are contributing to long-term success in improving foreign nations' ability to more effectively combat cybercrime.

Recommendation for Executive Action

The Secretary of State should instruct the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs to conduct a comprehensive evaluation of capacity building efforts to counter cybercrime. (Recommendation 1)

Agency Comments

We provided a draft of this report to the Departments of Homeland Security, Justice, and State for review and comment. We received and incorporated technical comments from the Departments of Homeland Security and Justice, as appropriate.

In its written comments, which are reproduced in appendix IV, State concurred with our recommendation to conduct a comprehensive evaluation of capacity building efforts to counter cybercrime.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Homeland Security and State, and the Attorney General. In addition, this report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov, or Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Kevin Walsh
Director, Information Technology and Cybersecurity

Latesha Love-Grayer
Director, International Affairs and Trade

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe challenges in building global capacity to combat cybercrime, and (2) determine actions selected federal agencies are taking to build foreign nations' capacity to combat cybercrime and the extent to which they are evaluating the effectiveness of their efforts.

To address the first objective, we analyzed plans, strategies, and our prior reports to identify potential relevant federal agencies that provide assistance aimed at building foreign nations' capacity to combat cybercrime. Based on our analysis, we identified seven federal agencies that may provide assistance focusing on building foreign nations and international criminal justice entities' ability to combat cybercrime. The agencies identified were the Departments of Commerce, Defense, Homeland Security (DHS), Justice (DOJ), State, and the Treasury, and the Federal Communications Commission.

We interviewed officials from the seven federal agencies to determine what activities to build capacity to combat cybercrime they provide, if any, and the component entities responsible for providing this assistance. After interviewing officials from the agencies and analyzing evidence they provided related to activities to build capacity to combat cybercrime, we determined that three agencies provide the majority of U.S. assistance in this area. Specifically, DHS, particularly its U.S. Immigration and Customs Enforcement and U.S. Secret Service; DOJ, particularly its Criminal Division and Federal Bureau of Investigation; and State, particularly its Bureau of International Narcotics and Law Enforcement Affairs.

We interviewed DHS, DOJ, and State officials to understand challenges, if any, they face in providing capacity building activities to foreign nations and international criminal justice entities. We compiled the challenges identified during various meetings with agency officials. We then had officials from each agency confirm if they agreed or disagreed with the challenges.

We also convened a panel of experts from international entities that have done work focusing on international cooperation and capacity building to combat global cybercrime. We conducted outreach to 12 international

entities and had seven experts participate in the panel. The panel included the following experts:[1]

- Carmen Corbin, Head of Counter Cybercrime Programming for West and Central Africa, United Nations Office on Drugs and Crime
- Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Center
- Chris Painter, President, Global Forum on Cyber Expertise
- Denise Mazzolani, Deputy Head of the Strategic Police Matters Unit – Transnational Threats Department, Organization for Security and Cooperation in Europe
- Mark Williams, Practice Manager for Digital Development Global Practice, World Bank
- Nick Beecroft, Nonresident Scholar in the Technology and International Affairs Program, Carnegie Endowment for International Peace
- Rodrigo Silva, Senior Legal Officer in the Department of Legal Cooperation of the Secretariat for Legal Affairs, Organization of American States

We asked the panelists to provide their perspectives on our definition and four categories of capacity building to combat cybercrime, and if there were any points we should consider adding. Additionally, we presented the challenges that DHS, DOJ, and State identified when providing capacity building assistance to foreign nations. We asked the panelists for their perspectives on the identified challenges, conducted a poll to determine the top two challenges, and discussed actions that individual entities and countries could take to work towards mitigating the top two challenges.

We also asked the panelists to identify their biggest challenges in working with the U.S. government in ongoing efforts to help combat international cybercrime. Last, we asked the panelists to identify the most critical action an individual entity or government can take to help combat international cybercrime. We obtained permission from each expert participant to record and transcribe the panel.

Following the panel, we analyzed the transcript using a content analysis methodology. One reviewer summarized the main points from the panel

[1]The panelists' titles and entities listed reflect their titles and entities when we convened the panel in November 2021.

transcription into overarching themes and recurring points, and consolidated the groupings into a coding index of categories. After the first reviewer coded the entire transcription, the second reviewer noted either agreement or disagreement with the first reviewer's codes. In instances where the reviewers disagreed, they would discuss their rationale and adjust the coding until they reached an agreement.

Through the content analysis, we identified similar challenges that State, DOJ, and DHS officials, as well as expert participants face when assisting foreign nations and international criminal justice entities. We presented to State, DOJ, and DHS officials, the challenges that the experts highlighted in working with the U.S. and provided the officials the opportunity to comment on the challenges.

To address the second objective, we analyzed numerous documents from various international entities that discuss capacity building to combat cybercrime. We compiled definitions from various sources, including Council of Europe, *Global Project on Cybercrime–Capacity Building on Cybercrime;* Organization for Security and Cooperation in Europe, *Crime in the Digital Age–Enhancing Capacities of Criminal Justice Institutions across the Organization for Security and Cooperation in Europe Area;* Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations;* World Bank, *Combatting Cybercrime–Tools and Capacity Building for Emerging Economies*; and United Nations Office on Drugs and Crime, draft *Comprehensive Study on Cybercrime*. We used these reports and entities' definitions to help develop our definition of capacity building to combat cybercrime, and to identify categories of, and develop definitions for, activities to build capacity to combat cybercrime. We identified categories through research on the types of assistance entities provide to combat global cybercrime and determined that assistance could be grouped into four categories.

We used a data collection instrument to gain DHS, DOJ, and State officials' perspectives on our definition and four categories of capacity building to combat cybercrime. We also reviewed agencies' responsibilities and obtained documentation for the various activities they have completed to build foreign nations' and international criminal justice entities' capacities to combat cybercrime. We analyzed this information and summarized and grouped each activity into one of our four categories of capacity building to combat cybercrime.

We also analyzed the International Telecommunication Union's *2020 Global Cybersecurity Index* to understand the 194 participating countries' commitments to cybersecurity. To select a manageable number of countries, we first identified four of the participating countries that are

members of the Budapest Convention and have a Global Law Enforcement Network presence. We then selected 30 participating countries, including the top five scoring countries for each of the six identified regions from the report's global competitiveness index scores.

We then requested from State the integrated country strategies for the 34 countries selected from the global cybersecurity index. We selected 10 of the 34 integrated country strategies for further analysis: the four countries that are members of the Budapest Convention and have a Global Law Enforcement Network presence, and one of the top five scoring countries from each of the six regions. To select one country from each of the six regions, we first analyzed the integrated country strategy for the country with the highest score and determined if it included any priorities related to combatting cybercrime. If it did, we selected that integrated country's strategy; if it did not, we moved consecutively down the list of the top five until we identified an integrated country strategy that included such priorities. We conducted follow-up with the agencies identified in the 10 integrated country strategies as having roles in executing the priorities related to combatting cybercrime and determined how they execute and evaluate their tasks.

We also analyzed program documents, such as interagency agreements, that detailed the federal agencies' capacity building activities, and the supporting evidence that outlined the outcome of select activities and projects. We later interviewed agency officials to understand how they determine if individual activities and overall capacity building efforts are achieving intended objectives, and how the agency determines if overall efforts were effective or led to successes or institutional change in foreign nations.

We compared agency documentation against requirements established by the GPRA Modernization Act of 2010. Specifically, we determined if agencies had strategic plans with goals that described how they contribute to agency priorities and how the goals were to be achieved. Additionally, we determined if agencies had established performance indicators to be used in monitoring progress towards goals, including output and outcome indicators. Further, we compared State's outputs and outcomes against department requirements for program performance and evaluations, and determined the extent to which agency documents met evaluation requirements.

We conducted this performance audit from January 2021 to March 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: State's, DOJ's, and DHS's Strategic Plans

The Departments of State, Justice (DOJ), and Homeland Security (DHS) outline priorities and goals for building international capacity to combat cybercrime in their strategic plans.

State's Joint Strategic Plan documents the department's priorities to promote international security and work with allies and partners to deter adversaries and counter transnational threats.[1] State's goals include:

- sustaining and enhancing international cooperation to promote U.S. objectives of an open, interoperable, reliable, and secure internet and cyberspace; and
- strengthening the capacity of the U.S. and partner nations to detect, deter, mitigate, and respond to international cyber threats and incidents.

DOJ's strategic plan highlights the department's objectives to protect national security and fight cybercrime, which requires countering cyber threats from foreign and domestic actors.[2] According to the plan, the department aims to:

- deter and disrupt cyber threats, and prosecute lone actors and transnational criminal organizations;
- strengthen interagency, intergovernmental, international, and private sector partnerships;
- safeguard department systems through training and personal security measures to deter and prevent internal and external threats; and
- enhance cyber resilience outside the department through information and intelligence sharing with the private sector and other government organizations.

Further, the plan notes that DOJ's goals are to increase:

- disruptions of malicious cyber actors' use of online infrastructure;

[1]Department of State and U.S. Agency for International Development, *Joint Strategic Plan FY 2022-2026* (March 2022).

[2]Department of Justice, *Strategic Plan FY 2022-2026* (July 2022).

- reported ransomware incidents from which cases are opened, added to existing cases, or resolved or investigative actions taken; and
- operations conducted jointly with strategic partners.

DHS's strategic plan outlines the department's objectives to secure cyberspace and critical infrastructure, including combatting cybercrime by disrupting and dismantling criminal organizations and expanding multilateral cooperative agreements with international partners.[3] The strategic plan highlights DHS's goals to hold cybercriminals accountable and reduce cybercrime through focused law enforcement activity and public-private partnerships. To achieve these goals, the department is to:

- investigate cybercrimes targeting individuals, private organizations, and public interests;
- engage in joint or collaborative investigations and provide voluntary cyber investigative assistance to law enforcement partners both domestic and foreign; and
- participate in information and intelligence sharing with stakeholders to prevent and disrupt criminal schemes involving cyberspace.

[3]Department of Homeland Security, *Strategic Plan FY 2020-2024* (July 2019).

Appendix III: Expert Panel

In November 2021, we convened a panel with experts from seven international entities that have done work focusing on international cooperation and capacity building to combat global cybercrime. The panelists consisted of the following:[1]

- Carmen Corbin, Head of Counter Cybercrime Programming for West and Central Africa, United Nations Office on Drugs and Crime
- Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Center
- Chris Painter, President, Global Forum on Cyber Expertise
- Denise Mazzolani, Deputy Head of the Strategic Police Matters Unit – Transnational Threats Department, Organization for Security and Cooperation in Europe
- Mark Williams, Practice Manager for Digital Development Global Practice, World Bank
- Nick Beecroft, Nonresident Scholar in the Technology and International Affairs Program, Carnegie Endowment for International Peace
- Rodrigo Silva, Senior Legal Officer in the Department of Legal Cooperation of the Secretariat for Legal Affairs, Organization of American States

Experts' Views on GAO's Definition and Four Categories of Capacity Building to Combat Cybercrime

We presented the panelists our original definition of capacity building to combat cybercrime, and asked them to provide their perspectives on our definition and if there were any points we should consider adding. The original definition was: assist in fostering responsible cybersecurity culture and enhancing international cooperation, creating effective legal and regulatory frameworks through collaborations between public and private sectors and international entities, developing internationally accepted

[1]The panelists' titles and entities listed reflect their titles and entities when we convened the panel in November 2021.

policies and strategies, and enhancing cybersecurity knowledge through sustainable cybercrime training.[2]

Panelists highlighted a few points to consider:

- **Differentiating cybersecurity and cybercrime.** Combatting cybercrime involves the tools for investigation and digital evidence, the knowledge of how to preserve and process digital evidence, and the understanding of how to present it in a trial. Cybersecurity involves the hardening and protection of systems, preventing attacks, and creating the robustness to prevent attacks.
- **Incorporating prevention and resilience.** The number and quantity of cybercrime cases is not possible to address, but all capacity building should include prevention. Recognizing that it is not possible to stop every cybercrime and organizations at every level cannot be expected to prevent every form of cyberattack or cyber incident, resilience is essential.
- **Considering ability of a country to deal with cybercrime.** Cybercrime crosses borders and involves many legal and criminal justice systems working together, so effective international cooperation is essential. This includes building institutions and capacity in developing countries so they are able to deal with cybercrime in their countries and work with other jurisdictions who are helping them.
- **Fostering responsible cybersecurity culture.** This is important not only at the country level, but across governments, society, and at the individual user level.
- **Raising awareness of potential victims.** Efforts should include informing the general population and helping the private sector regarding staying aware of risks, protecting individuals or businesses, and reporting cybercrimes. It is essential for individuals and businesses to know how and where to report incidents.

Additionally, we presented our graphic which details the four categories of capacity building to combat cybercrime. We asked panelists for reactions and examples of actions that their entities were taking that related to each of the categories. Panelists noted that the four categories were generally scoped appropriately, and highlighted a few examples of their efforts:

[2]We revised our definition of “capacity building to combat cybercrime” after we presented it in November 2021, in part, due to the panelists’ comments. Our final definition is reflected in the background of this report.

Cooperation and communication

- One expert noted that the entity utilizes trained experts in a certain country to train neighboring countries, and creates networks between countries that participate in capacity building workshops. The idea is that countries can continue to grow their knowledge by working together. For example, this entity used trained digital evidence experts in Senegal to help and offer training in Niger. In addition, it established working relationships between the cyber units in Burkina Faso, Niger, and Senegal.
- Another expert stated that the country brings participants from various workshops into a shared space to exchange information and contacts, highlighting the benefits of mutual legal assistance.

Legal

- A few experts noted that they encourage countries to create strong laws and adopt legal tools, particularly the Budapest Convention.

Policy and strategy

- A couple of the experts noted that they encourage participating states to adopt national strategies and action plans, particularly with a cybercrime component embedded in it.
- One expert stated that the entity looks at countries' policies and strategies with a cybercrime component and tries to develop best practices from each to be shared internationally.

Training and technical assistance

- One expert noted that the country trains investigators and first responders on cybercrime incidents, and provides legal training on the Budapest Convention.
- Another expert stated that the country has conducted in-depth assessments for the police academy and judicial academy to determine if their training curriculum needs to be upgraded or amended.

Critical Actions Organizations and Governments Can Take to Help Combat Global Cybercrime

We asked the panelists to share one critical action their organizations could take to help combat cybercrime. Panelists highlighted that entities should:

- Provide training specific to countries' needs to make it sustainable

- Continue offering assessments to ensure countries understand where their gaps and vulnerabilities exist
- Assemble stakeholders from developing countries to raise global awareness and establish priorities
- Enhance the capacities of the entire criminal justice system to process and resolve cybercrime cases
- Make cyber issues and cyber-related risks a key component of every aspect and project of an organization, rather than a partitioned area
- Convene stakeholders who may have opposing views on the challenge to help facilitate common action in a confidential setting
- Aim to be flexible and react quickly to address emerging issues, such as ransomware, in trainings and workshops

We also asked the panelists to share one critical action governments could take to help combat cybercrime. Panelists highlighted that governments should:

- Prioritize combatting cybercrime and put sufficient resources behind it, such as specialized law enforcement units as well as prosecutors and judges who understand the issues
- Prioritize cybercrime and engage with and seek support from developing countries
- Prioritize going after safe havens for cybercriminals in countries that either cannot or will not investigate and punish cybercrime
- Create a well-coordinated national system that encompasses not only law enforcement and their capabilities, but judiciary and education and their capacities to respond swiftly to requests from abroad
- Encourage a perspective change regarding the risk cybercrime poses: it affects all levels, including developing nations and not just wealthier countries
- Impose costs on criminal actors to signal that there are unacceptable behaviors that will be punished
- Prioritize investigating cybercrimes as well as prosecuting and convicting cybercriminals

Appendix IV: Comments from the Department of State

United States Department of State
Comptroller
Washington, DC 20520

FEB 17 2023

Jason Bair
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Bair:

We appreciate the opportunity to review your draft report, "GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime" GAO Job Code 104768SU.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

James A. Walsh

Enclosure:
As stated

cc: GAO – Latesha Love
INL – Todd Robinson
OIG - Norman Brown

Department of State Comments on Draft GAO Report

GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime
(GAO-23-104768SU, GAO Code 104768SU)

Thank you for the opportunity to comment on the GAO draft report, *GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime.*

Recommendation 1: The Secretary of State should instruct the Assistant Secretary of State's Bureau of International Narcotics and Law Enforcement Affairs to conduct a comprehensive evaluation of capacity building efforts to counter cybercrime.

The Department concurs with the recommendation. INL will conduct an independent internal evaluation of capacity building efforts to counter cybercrime. A social scientist from INL's Office of Knowledge Management will work with the program team in the Office of Global Policy and Programs to evaluate the extent to which the overall program and related projects have achieved their expected results, and to make recommendations as needed.

Accessible Text for Appendix IV: Comments from the Department of State

FEB 17 2023

Jason Bair
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Bair:

We appreciate the opportunity to review your draft report, "GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime" GAO Job Code 104768SU.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

James A. Walsh

Enclosure:
As stated

cc: GAO-Latesha Love
INL-Todd Robinson
OIG - Norman Brown

Department of State Comments on Draft GAO Report

GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime
(GAO-23-104768SU, GAO Code 104768SU)

Thank you for the opportunity to comment on the GAO draft report, GLOBAL CYBERCRIME: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime.

Recommendation 1: The Secretary of State should instruct the Assistant Secretary of State's Bureau of International Narcotics and Law Enforcement Affairs to conduct a comprehensive evaluation of capacity building efforts to counter cybercrime.

The Department concurs with the recommendation. INL will conduct an independent internal evaluation of capacity building efforts to counter cybercrime. A social scientist from INL's Office of Knowledge Management will work with the program team in the Office of Global Policy and Programs to evaluate the extent to which the overall program and related projects have achieved their expected results, and to make recommendations as needed.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Kevin Walsh at (202) 512-6151 or walshk@gao.gov
Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Kush K. Malhotra (Assistant Director), Rob Ball (Assistant Director), Paige Teigen (Analyst in Charge), Joshua Akery, David Ballard, Chris Businsky, Mark Dowling, Becca Eyler, Hiama Halay, Franklin Jackson, Igor Koshelev, Ashley Mattson, Jonah Silencieux, and Andrew Stavisky made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548