THIRD WAY

MEMO *Published October 1, 2019 • 21 minute read*

The Need for Better Metrics on Cybercrime

Ishan Mehta
Policy Advisor, National Security Program
@ishan_tweeting

Takeaways

The United States is facing a massive cybercrime wave, yet there are no comprehensive statistics available on the size and scope of the problem and law enforcement's actions against it. Without these statistics, it is difficult to make an informed case for policy changes to reduce the cybercrime wave and bring cybercriminals to justice.

There are three major buckets of data that do not currently exist in the United States in full that policymakers need to address: 1) the magnitude and costs of cybercrime, 2) the extent of law enforcement efforts to counter cybercrime, and 3) the impact of these law enforcement efforts in reducing cybercrime.

This memo details the current state of cybercrime metrics and recommends Congress take the following actions to address the gaps in available data:

1. Establishing a Baseline: Require the Federal Bureau of Investigation (FBI) and the Department of Justice

(DOJ) to report data that these entities already collect (or did collect) on cybercrime but is no longer made public. This includes:

- Releasing arrest numbers for cybercrime in the annual incident-based reporting data released by the FBI.
- Publishing data as part of the FBI's annual Internet Crime Complaint Center (IC3) reports that assesses perpetrators of cybercrime in cases investigated by the FBI.
- Reinstating an updated DOJ Bureau of Justice Statistics' (BJS) National Computer Security Survey, which is a private sector survey on cybercrime.

2. Reforming Incident Data Systems: Advance legislation that takes into account the recommendations laid out by The National Academies of Sciences, Engineering, and Medicine (NAESM) in 2018. These recommendations would establish a new crime incident reporting system that measures the harm caused by cybercrime.

3. Evaluating Success: Ask the Government Accountability Office (GAO) to study the current mechanisms that the U.S. government uses to measure and evaluate the effectiveness of its efforts to reduce crime and their effectiveness and applicability to cybercrime.

There is a cybercrime wave in the United States but we can't measure it.

The United States is facing a cybercrime wave that threatens America's economic and national security. America's cybercrime wave has targeted every sector of the U.S. economy and hit state and local governments across the country. Yet, we neither have substantial metrics to measure the extent of this problem nor an assessment of the efforts taken to counter it.

Just in the summer of 2019, the City of Baltimore, the Georgia courts system, and Lake City, Florida were the victims of ransomware where hackers deny access to users' own computers until a ransom is paid. Malicious cyber actors have attacked health care systems and critical infrastructure in the United States, such as Industrial Control Systems (ICS) and the electric grid. [1] Academics have estimated that about half of all property crime is now cybercrime. [2]

There is limited data on the size and scope of the cybercrime wave. There were over 350,000 cybercrime incidents reported to the FBI in 2018, a 16% increase from the year before. [3] The White House Council of Economic Advisers estimated in 2016 that malicious cyber activity costs the U.S. economy up to $109 billion annually. [4] Law enforcement has not done enough to counter this malicious activity, allowing cybercriminals to continue to operate with impunity. Third Way's analysis of publicly available data estimates that less than 1% of cyber incidents see an arrest of the perpetrator, recognizing that this data is incomplete. [5]

Cybercrime data has been unreliable and inconsistent across government agencies. There is also reason to believe that the numbers the government releases on cybercrime rates are severely underreported. A Gallup poll from 2018 showed that one in four American households have experienced cybercrime in the previous year. [6] That is exponentially larger than the number of cybercrime incidents reported annually by the FBI. Additionally, other estimates have shown the cost of cybercrime to be much higher than the 2016 White House estimate with some saying that cybercrime costs up to a trillion dollars. [7] While these private sector reports have

their own methodological challenges and should not be taken at face value, they are given credence because the U.S. government does not have comprehensive metrics of its own.

Without metrics on the rate of cybercrime, the law enforcement actions taken against cybercriminals, and the impact these actions have on combating the threat, it will continue to be difficult for policymakers to make decisions about needed policy changes in order to assess the adequacy of current public policy approaches. To make progress in the fight against cybercriminals, there needs to be an extensive assessment of current government efforts across all agencies to determine what is working, what can be amplified, and what needs to change.

There is a cybercrime wave in the United States but we can't measure it.

There are three major buckets of cybercrime data that need to be improved: 1) the size and cost of the cybercrime problem, 2) the extent of law enforcement efforts to counter cybercrime, and 3) the impact these law enforcement efforts have in reducing cybercrime.

1. Measuring the size and cost of the problem

If we don't understand the pervasiveness and cost of the cybercrime wave, it is impossible to know if our efforts are adequate. Unfortunately, the U.S. government does not collect and report consistent metrics on the magnitude and impact of cybercrime in the United States. This includes the number of cybercrime incidents that hit victims in the country and their costs to them. We need to count every victim of a crime. Without proper statistics to count the number of incidents, we do not know as a society how big a problem cybercrime is. Without metrics for costs, we do not know the impact of these crimes.

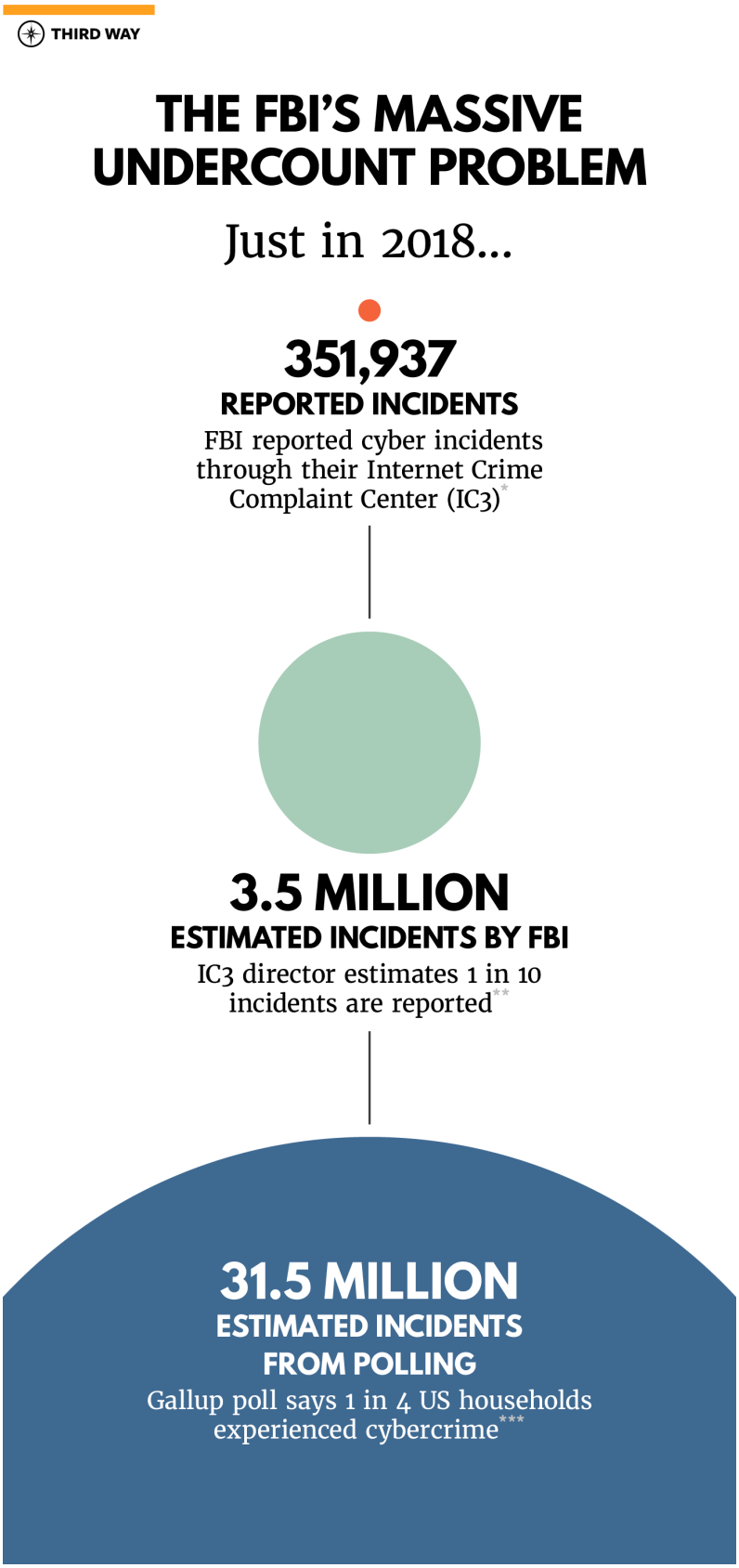
Unfortunately, the U.S. government does not collect and report consistent metrics on the magnitude and impact of cybercrime in the United States.

TWEET THIS

Measuring the size of the cybercrime wave

The U.S. government admits that the data it collects on cybercrime incidents annually is an undercount. The FBI's IC3 program releases annual reports that include the number of cyber incidents in the United States. [8] However, this number only includes the incidents that are self-reported by victims through the IC3's online portal. By the IC3's own estimate, this number only represents 10-12% of the total number of incidents in the country because most victims do not report their victimization. [9] However, non-government sources show this problem to be larger. Gallup found that one in four households were a victim of cybercrime in 2018. If that poll is accurate, it would mean that the FBI collects about 1 in 90 of all cybercrime incidents in its IC3 database.

THIRD WAY



The government is not reporting all the data it possesses. Multiple federal agencies also collect crime complaints through other means but do not report numbers publicly. For

example, iGuardian is a secure portal allowing FBI partners within criticall telecommunications, defense, banking and finance, and energy infrastructure sectors to report cyber incidents to the FBI in real time. [10] Yet, there is no public reporting of this number. Similarly, there is no consolidated number for the incidents reported to the Secret Service or other federal law enforcement agencies. This is despite the fact that the *Uniform Federal Crime Reporting Act of 1988* (P.L. 100-690) [11] compels federal law enforcement agencies to report nationwide criminal statistics to the FBI. [12]

The government is trying to improve its data collection efforts, but the planned fix isn't enough. The National Incident Based Reporting System (NIBRS), which was first approved for use in 1988, [13] would lead to more accurate reporting across all levels of America's law enforcement agencies, including state and local, but these agencies have been slow to report into it. NIBRS is replacing the older Unified Crime Reporting (UCR) system administered by the FBI and designed to capture reporting from federal, state, and local law enforcement agencies on the number of crime incidents in the United States across a number of categories and details about these crimes such as known information about victims and offenders. Prior to this, the UCR only collected federal crime data. However, only a fraction of state and local law enforcement agencies are reporting into NIBRS. Currently, less than half of the total 17,985 state and local law enforcement agencies identified by the President's 21 st Century Policing Report do so. [14] Those agencies that have reported into NIBRS represent 105 million citizens in the United States, less than one-third of the total population. Currently, NIBRS does not have reporting for the crime incidents that affect the other 250 million citizens in the United States

Underreporting by both individual victims and private sector victims is a real issue hindering the collection of reliable cybercrime data. The IC3 estimates only about 10 to 12% of cybercrimes are reported through their portal. [15] DOJ has said that only one in six fraud victims report to law

enforcement. [16] There are multiple reasons why this underreporting takes place. Victims may not believe that they will get restitution by reporting to law enforcement, or may not know how or to whom to report. Corporations are also victims of cybercrime and may be incentivized to not report to law enforcement. Corporations fear reputational and financial damage that often follows disclosing victimization of a cyber incident. Litigation costs and fines can be larger than the direct cost of mitigating the incident. [17] Considering these factors, it is not surprising that organizations that were hacked by China to steal intellectual property were reluctant to identify themselves as victims and cooperate with the U.S. government. [18] The crimes that are not counted still have an economic and social impact, and it is important that we establish mechanisms to understand their impact.

The crimes that are not counted still have an economic and social impact, and it is important that we establish mechanisms to understand their impact.

Surveys of crime victims are one method of capturing more accurate data on the size and scope of the problem, but the current surveys implemented by the U.S. government do not capture cybercrime incidents. For example, the National Crime Victimization Survey (NCVS) is an annual household survey of the United States that covers 95,000 households and is conducted by DOJ's BJS. [19] The survey is anonymized which encourages disclosure of victimization for crimes that individuals are reluctant to report to law enforcement, such as sexual assault or fraud. As identified by the 2017 GAO report on Cost of Crime, the NCVS does not report on cybercrime. [20] It does report on identity fraud, which may happen online, but is only one of many types of cybercrime.

At the private sector level, anonymized surveys allow corporations to be counted as victims without fearing any further damage, but federal surveys of this kind have been discontinued. BJS' National Computer Security Survey, last conducted in 2005, surveyed over 7,000 businesses in the United States and found that over two-thirds had been a victim of cybercrime that year. [21] Although the survey did not have a great response rate, the survey also found that most businesses did not report these incidents to any law enforcement authority. Considering the trajectory of technology and crime, it is likely that this number would be much higher if such a survey were conducted today, which would help to fully understand the impact of cybercrime on the corporate sector.

Measuring the cost of cybercrime

To develop adequate and efficient policy solutions to tackle cybercrime, it is crucial to understand the societal harm it inflicts. An accurate assessment of the cost of cybercrime would draw attention to the issue and create political will to act on it. The current numbers reported by the FBI through IC3 are in conflict with numbers reported from other studies. The 2018 annual IC3 reported that cybercrime cost $2.71 billion in victim losses in 2018. [22] However, this does not take into account the indirect losses from the incident. [23] The White House Council of Economic Advisers estimate the total cost to the U.S. economy is between $57 and $109 billion. Other private sector studies put this amount much higher. [24]

Adapting a harm-based approach for collecting incident data would allow policymakers to tally the cost from individual incidents and present a more accurate picture of the overall impact of cybercrime on commerce and the economy.

Unfortunately, current efforts by law enforcement to collect information on the cost of cybercrime remain inadequate. The 2016 study by the White House Council of Economic Advisors identified several gaps in data collection that hindered their collection. [25] A GAO study on the Cost of Crime in 2017 identified cybercrime as a category of crime not covered in the FBI's index for calculating the costs of crime. [26] The report further stated that "cybercrime may occur frequently and could pose significant societal costs, but systematic information on these types of crimes is not available." Adapting a harm-based approach for collecting incident data would allow policymakers to tally the cost from individual incidents and present a more accurate picture of the overall impact of cybercrime on commerce and the economy.

Even if all federal, state, and local law enforcement agencies report into NIBRS incidents of cybercrime and other forms of crime, that alone is not sufficient to assess the full impact of these crimes on victims, especially the cost. The National Academies of Sciences, Engineering, and Medicine (NASEM), a non-profit entity established by Congress in 1863, has recommended a data collection framework modeled off of one recommended by the United Nations that would allow for more detailed reporting on different types of cybercrime and other forms of crime beyond what is collected through NIBRS. [27] The report also states that "the nation's crime statistics will remain inadequate unless they expand to include more than just simple tallies with no associated measure of uncertainty or capacity for disaggregation." [28] The authors advocate for including important measures related to an offense, particularly on the harm caused to victims of each incident such as direct or indirect losses from a crime. These different measurements would help understand the full impact of crime incidents beyond just that they occurred. [29] While the recommendations in the report are relevant for all crime, they are particularly applicable to cybercrime. In NIBRS, a ransomware attack which can shut down an entire hospital or

city administration would be given an offense count of one. That does little to convey the impact of what actually happened. A new crime data infrastructure that takes a harm-based approach would help understand the real world impact and cost of these crimes.

2. Measuring the extent of law enforcement efforts against cybercrime

The U.S. government does not currently have a comprehensive mechanism in place across government agencies to measure the extent of law enforcement efforts against cybercrime. Only law enforcement in the United States can actually impose consequences on the human actor behind cybercrime. Measuring these efforts allow us to examine the effectiveness of current policies and strategies. They also let policymakers assess if the current level of resources committed to deal with cybercrime are adequate and utilized efficiently.

One data point used to measure law enforcement effectiveness in bringing criminals to justice is clearance rates. Law enforcement agencies can clear an offense by arrest or by exceptional means such as the death of the offender. These clearance numbers can then be reported as a clearance rate, which allows the public to see how many cases were closed versus the total number of incidents reported in a given year. This rate allows the public to determine the extent to which law enforcement is making progress in bringing criminals to justice. [30] While the old Unified Crime Reporting (UCR) system did not separate out clearances by arrest or exceptional means, NIBRS does allow for this much more detailed data. [31]

Although federal law enforcement agencies are required to report crime and arrest data through the FBI by the *Uniform Federal Crime Reporting Act* (P.L. 100-690) [32] , many do not do so. [33] That is in stark contrast to the sophisticated reporting on other types of property crime such as arson or motor-vehicle theft where NIBRS reports the number of incidents,

incidents cleared by arrest, and cleared by exceptional means. [34] In the memo, "Reader's Guide to Understanding the U.S. Cyber Enforcement Architecture and Budget", Third Way has identified close to 20 law enforcement agencies in the federal government that take enforcement action against malicious cyber activity. [35] Most of these agencies provide no metrics on their activities. While this paper will not delve into the reporting structures of each one of them, certain law enforcement agencies have reported out individually specific metrics on their efforts. The FBI used to report the number of arrests made for cybercrime from each field office but discontinued this practice after 2015. [36] Only the Secret Service's numbers are representative of the entirety of their efforts. The Secret Service reports the number of annual arrests made for cyber related offenses and the potential losses prevented. [37] The reports do not provide a methodology for how these losses are calculated. The FBI, in their annual Congressional Budget Justification, provides some information regarding their activities to counter cybercrime but is less detailed. The FBI reports the number of convictions for Internet fraud and the number of "high-impact" Internet fraud targets neutralized. [38] Internet fraud does not cover all areas of cybercrime that the FBI prosecutes and there is no definition of what "high-impact" targets are or what neutralized refers to. The FBI uses a similarly vague term, "disrupted," to deal with counterterrorism cases that has been criticized by civil liberties groups. [39]

Federal, state, and local law enforcement agencies are responsible for the protection of the citizens of the United States. Collectively they spend billions of dollars to fulfill this mandate each year. An accurate measure of their efforts to counter cybercrime is required for policymakers to judge the effectiveness of current strategies and the efficiency of the current resources allocated. Without an effective and efficient approach, no progress can be made in the fight against cybercrime.

3. A long-term benchmark: defining success in the fight against

cybercrime.

Along with measuring the size of the cybercrime problem and the efforts to reduce it, there is not currently a mechanism in place to evaluate the impact of these efforts across the U.S. government. Former Deputy Attorney General Rod Rosenstein has admitted publicly that he grappled with the question of "measuring success" on a daily basis. [40] There has not been a dedicated effort across government agencies to determine what metrics should be used to monitor and evaluate how well law enforcement is doing in punishing and deterring malicious cyber actors.

An important component of evaluating government efforts against cybercrime is the establishment of success metrics. Currently, the FBI and DOJ lack comprehensive performance metrics that set targets for cybercrime and measure how well they are doing in reaching those targets. For other categories of crime, such as organized crime and white collar crime, the FBI sets targets like cases cleared or dollar amounts recovered. [41] None of DOJ's 12 long-term performance measures mention cybercrime. [42] In the federal government, only the Secret Service sets targets for each year, reported to Congress, on a number of cyber-related measures. This includes the amount of dollar-loss prevented by Secret Service cyber investigations as well as the number of law enforcement officials trained in cybercrime and cyber forensics. [43]

None of DOJ's 12 long-term performance measures mention cybercrime.

While success metrics can serve as useful benchmarks, they can also have unintended consequences. As the 9/11 Commission documented in the terrorism context, case targets can often set up skewed incentives to take on easy, low-impact cases instead of targeting the most critical cases that may be more complicated. [44] We do not know the best

way to set targets for law enforcement in cybercrime. There may be lessons to be learned from criminology studies in other areas of crime that are similar to cybercrime. Proceeding to do so without doing our due diligence could lead to more harm than good. More work is required to understand the best way to move forward that is beyond the scope of this memo.

Congress can take a number of actions to improve the state of cybercrime metrics.

Congress has an important oversight role over America's law enforcement agencies, which are currently lacking the mechanisms and abilities to collect critical data on cybercrime. In the past, major changes in crime data collection in the United States have come from congressional action. Congress needs to act once again to reform crime data collection to adapt them for the 21 st century in which a large majority of crimes have a digital nexus to them. The following recommendations provide Congress a path to ensure the United States has robust metrics to assess how well the government is doing against the burgeoning cybercrime wave.

The first set of recommendations help establish a baseline on the size and scope of cybercrime in the United States and boost the reporting of data that law enforcement agencies already possess but have either never disclosed or discontinued its collection. The second set of recommendations focus on reforming the current crime data collection systems and infrastructure to allow for more detailed reporting on cybercrime efforts. The final recommendation focuses on evaluating the success of law enforcement efforts against cybercrime.

1. Establishing a baseline

Congress should require the FBI and DOJ to report data that these entities already

collect (or did collect) on cybercrime but is no longer made public. This includes:

Releasing arrest numbers for cybercrime in the annual incident-based reporting data released by the FBI.

The *Unified Crime Reporting Act of 1988* (P.L. 100-690) [45] requires all federal law enforcement agencies to report crime data through the FBI. Yet, some of these agencies have never reported these numbers to the FBI. [46] Currently, state and local law enforcement agencies are beginning to report crime data through the NIBRS system that allows for more detailed information to be distilled about crimes that occur in the United States, including cybercrime. However, federal agencies, including the FBI and Secret Service, are not doing the same. Congress should call on DOJ to assess why all 20 federal law enforcement agencies tasked with enforcing cybercrime, including the FBI and its smaller programs like IC3 and iGuardian, do not report arrest, incident data, and clearance rate for cybercrime through NIBRS. Congress should also increase funding to the DOJ's state and local grant-making program to ensure more state and local agencies adopt NIBRS.

Publishing data as part of the FBI's annual IC3 reports that assesses perpetrators of cybercrime in cases investigated by the FBI.

Congress should mandate that the IC3 return to the more detailed reporting it provided until 2009 on cybercrime cases that are self-reported by victims into the FBI system. This includes details on perpetrators of cybercrime for cases where the FBI has been able to investigate and identify the person(s) that committed a cybercrime. Additionally, the mandate should require the IC3 reports to provide data on the number of incidents that were investigated and led to an arrest or some form of enforcement action. This data should correspond to the NIBRS reporting as well.

Reinstating the DOJ Bureau of Justice Statistics' (BJS) National Computer Security Survey, which is a private sector survey on cybercrime.

DOJ's BJS instituted a survey of the impact of cybercrime on private sector victim organizations from 2001 until 2005. It has since been discontinued. Congress should pass legislation to authorize BJS to develop a new improved survey instrument for the current day and ensure that the Commerce, Science, and Justice Appropriations bill provides sufficient funding for this to occur annually. This survey allows for the collection of anonymized cybercrime data from victim companies. In addition, Congress should also require that the National Crime Victimization Survey cover cybercrime, to collect anonymized cybercrime data from individual victims. Anonymized surveys would be able to collect incident data from victims that are reluctant to report for a variety of reasons.

2. Reforming Crime Data Reporting Systems:

Congress should advance legislation that takes into account the recommendations laid out by The National Academies of Sciences, Engineering, and Medicine (NASEM) in 2018. This includes:

Establishing a new crime incident reporting system that measures the harm caused by cybercrime.

Congress should take steps to move the United States towards a harm-based approach to collect crime data that allows the public to assess the impact of crimes on victims and better account for crimes that occur in the 21st century. NASEM in 2018 recommended this approach not only to improve more holistic reporting on cybercrime, but to improve the accuracy and utility of crime statistics in this country across all categories of crime. Before advancing legislation that adopts the recommendations of the 2018

NASEM report, Congress should request a GAO assessment on the feasibility of implementing a harm-based approach to the collection of crime data overall and particularly in the cases of cybercrime. This study could also assess the feasibility of implementing other harm-based crime reporting approaches specific to cybercrime, such as an approach used by the European Union. [47]

Additionally, Congress should host a series of hearings with experts in the field of crime reporting and cybercrime to better understand the gaps in the current system and their effect on understanding the full impact of cybercrime to help policymakers make more informed policy changes on how crime data is collected.

3. Evaluating Success and Future Research:

Congress should fund research to study the possible mechanisms that the U.S. government could adopt to measure and evaluate the effectiveness of its efforts to reduce cybercrime through law enforcement actions. This includes:

Leveraging the National Science Foundation and others to study cybercrime to understand the best way to define success.

Congress should work towards evaluating law enforcement's efforts against cybercrime and require them to eventually set targets that can measure the effectiveness of these efforts. To start, Congress can request GAO to conduct a study of the current mechanisms that the U.S. government uses to measure and evaluate the effectiveness against other types of crime and whether they would be applicable for cybercrime. Congress should also fund grants to study cybercrime through the National Science Foundation. This would include analyzing what performance targets could be established for different enforcement agencies to measure their efforts against these targets, being mindful to not set skewed

incentives that reward reaching these targets at the expense of pursuing more complicated and time-consuming cases.

Conclusion

To begin to make improvements in the government's ability to bring enforcement actions against cybercriminals, there must be a comprehensive assessment of current government efforts across all agencies with a role in cyber enforcement to determine what is working and what might need to change. Baseline statistics are required to make informed policy choices to mitigate the cybercrime wave. That baseline does not currently exist. Congress must work towards implementing the recommendations detailed in this memo on cybercrime metrics to: 1) establish a baseline, 2) reform crime reporting systems, and 3) evaluate the success of law enforcement efforts against the threat. Congress should engage law enforcement, the academic community, and the private sector in these discussions to ensure that we have comprehensive and robust metrics, which is the first step in the fight against cybercrime.

TOPICS

CYBERSECURITY 32

ENDNOTES

1. United States Department of Homeland Security. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." 15 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A. Accessed Oct. 3 2018.

2. Anderson, Ross, et al. *Measuring the Changing Cost of Cybercrime Our Framework for Analysing the Costs of Cybercrime*. pp. 1–32. https://informationsecurity.uibk.ac.at/pdfs/ABBCGGLMV2019_Measuring_the_Changing_Cost_of_Cybercrime_WEIS.pdf. Accessed 5 Aug 2019

3. Federal Bureau of Investigation. "2018 Internet Crime Report." 22 June 2018, pp. 5. https://pdf.ic3.gov/2018_IC3Report.pdf. Accessed 5 Aug. 2019.

4. United States White House, The Council of Economic Advisers. "*The Cost of Malicious Cyber Activity to the U.S. Economy.*" February 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 3 Oct. 2018.

5. Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." *Third Way*, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 6 Jun. 2019.

6. Reinhart, RJ. "One in Four Americans Have Experienced Cybercrime." *Gallup.com*, Gallup, 10 Dec. 2018, news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx. Accessed Aug. 5 2019.

7. Sterling, Bruce. "Global Cybercrime. Costs a Trillion Dollars. Maybe 3." *Wired*, Conde Nast, 19 July 2017, www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/. Accessed 3 Oct. 2018.

8. "Filing a Complaint with the IC3." *Internet Crime Complaint Center (IC3)*, Federal Bureau of Investigation, www.ic3.gov/. Accessed 5 Aug. 2019.

9. Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." *The New York Times*, The New York Times, 5 Feb. 2018,www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 5 Aug. 2018.

10. "Guardian." FBI, *Federal Bureau of Investigation*, 22 July 2016. www.fbi.gov/resources/law-enforcement/iguardian. Accessed 12 Feb. 2019.

11. 34 U.S. Code §%u202F41303 "All departments and agencies within the Federal government (including the Department of Defense) which routinely investigate complaints of criminal activity, shall report details about crime within their respective jurisdiction to the Attorney General in a uniform manner and on a form prescribed by the Attorney General" https://www.law.cornell.edu/uscode/text/34/41303

12. Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." *The New York Times*, The New York Times, 5 Feb. 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 5 Aug. 2018.

13. Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 58, doi.org/10.1111/1745-9133.12332. Accessed 5 Aug. 2019.

14. Office of Community Oriented Policing Services.. "Final Report of the Presidents Task Force on 21st Century Policing." *Final Report of the Presidents Task Force on 21st Century Policing*, 2015. https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf Accessed 30 Aug. 2019.

15. Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." *The New York Times*, The New York Times, 5 Feb. 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 5 Aug. 2019.

16. Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." *Police Executive Research Forum*, Jan. 2018. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf Accessed 5 Aug. 2019.

17. Ponemon Institute LLC. "2017 Cost of Data Breach Study, Global Overview." *IBM*, June 2017, pp. 1. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN. Accessed 5 Aug. 2019.

18. Sullivan, Laura, and Cat Schuknecht. "As China Hacked, U.S. Businesses Turned A Blind Eye." *NPR*, National Public Radio, 12 Apr. 2019, www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye. Accessed 5 Aug. 2019.

19. "Data Collection: National Crime Victimization Survey (NCVS)." *Bureau of Justice Statistics (BJS)*, Department of Justice, www.bjs.gov/index.cfm?ty=dcdetail&iid=245. Accessed 5 Aug. 2019.

20. United States, Congress, Government Accountability Office. "Costs of Crime, Experts Report Challenges Estimating Costs and Suggest Improvements to Better Inform Policy Decisions: Report to Congressional Requesters." GAO, Sept. 2017. www.gao.gov/assets/690/687353.pdf. Accessed 5 Aug. 2019.

21. "Cybercrime." *Bureau of Justice Statistics (BJS)*, Department of Justice (DOJ), www.bjs.gov/index.cfm?ty=tp&tid=41. Accessed 5 Aug. 2019.

22. Federal Bureau of Investigation. "2018 Internet Crime Report." 22 June 2018, pp. 5. https://pdf.ic3.gov/2018_IC3Report.pdf. Accessed 5 Aug. 2019.

23. A harms-based approach would also help understand the costs associated with cybercrime. As outlined by Anderson et al. in their paper, "Measuring the Changing Costs of Cybercrime", there are three categories of costs associated with cybercrime: 1) direct losses, 2) indirect losses, and 3) defense costs.[1] Direct losses are the costs to mitigate and recover from an incident. This can include the cost of data recovery, consultants, or ransoms paid to the attackers. Indirect losses are the result of reputational damages or fines levied by regulators for incident. Defense costs refer to the costs of implementing cybersecurity measures and training users. Direct losses and indirect losses are more relevant to calculate the cost from a single incident.

24. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

25. United States White House, The Council of Economic Advisers. "*The Cost of Malicious Cyber Activity to the U.S. Economy.*" February 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 5 Aug. 2019.

26. United States, Congress, Government Accountability Office. "Costs of Crime, Experts Report Challenges Estimating Costs and Suggest Improvements to Better Inform Policy Decisions: Report to Congressional Requesters." GAO, Sept. 2017. www.gao.gov/assets/690/687353.pdf. Accessed 5 Aug. 2019

27. Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 1075–98, doi.org/10.1111/1745-9133.12332. Accessed 5 Aug. 2019.

28. Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 10635–36, doi.org/10.1111/1745-9133.12332.

29. Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." *Criminology and Public Policy*, vol. 16, no. 4, 2017, pp. 4, doi.org/10.1111/1745-9133.12332. Accessed 5 Aug. 2019.

30. Cases are cleared by exceptional means in a few circumstances that include the death of the offender, victim's refusal to cooperate after an offender has been identified, or denial of extradition from another jurisdiction because the offender is being prosecuted in that jurisdiction. See "Clearances." *FBI: UCR*, Federal Bureau of Investigation, 10 Sept. 2018, ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/clearances. Accessed 5 Aug. 2019.

31. "Percent of Offenses Cleared by Arrest or Exceptional Means." *FBI:UCR*, Federal Bureau of Investigation, 14 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/tables/table-17. Accessed 5 Aug. 2019.

32. 34 U.S. Code §%u202F41303 "All departments and agencies within the Federal government (including the Department of Defense) which routinely investigate complaints of criminal activity, shall report details about crime within their respective jurisdiction to the Attorney General in a uniform manner and on a form prescribed by the Attorney General" See United States, Congress, *Uniform Federal Crime Reporting Act of 1988*. 1988. https://www.law.cornell.edu/uscode/text/34/41303. Accessed 5 Aug. 2019.

33. United States, Congress, House. United States Code. Title 34, section 41303, Legal Information Institute, 18 Nov 1988, https://www.law.cornell.edu/uscode/text/34/41303. Accessed 5 Aug. 2019.

34. "Percent of Offenses Cleared by Arrest or Exceptional Means." *FBI: UCR*, Federal Bureau of Investigation, 14 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/tables/table-17. Accessed 5 Aug. 2019.

35. Gaskew, Brandon. "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget – Third Way." *Third Way*, 21 Feb. 2019, www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget. Accessed 5 Aug. 2019.

36. "Federal Crime Data." *FBI:UCR*, Federal Bureau of Investigation, 16 Sept. 2016, ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/additional-reports/federal-crime-data/federal_crime_data_-2015. Accessed 5 Aug. 2019.

37. United States Secret Service, Department of Homeland Security. "Annual Report 2017.", pp. 16–17. https://www.secretservice.gov/data/press/reports/CMR-2017_Annual_Report_online.pdf. Accessed 5 Aug. 2019.

38. Federal Bureau of Investigation. "FY 2018 Authorization and Budget Request to Congress." May 2017, pp 4-29. https://www.justice.gov/file/968931/download. Accessed 5 Aug. 2019.

39. "Unleashed and Unaccountable." *ACLU.org*, American Civil Liberties Union, Sept. 2013, www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf. Accessed 5 Aug. 2019.

40. "Rosenstein Question." *C-SPAN*, 15 Apr. 2019, https://www.c-span.org/video/?c4792701/rosenstein-question. Accessed 30 Aug. 2019

41. Federal Bureau of Investigation. *FY 2018 Authorization and Budget Request to Congress*. Department of Justice. May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 19 Oct. 2018.

42. https://www.justice.gov/archive/mps/strategic2012-2016/appendixa.pdf

43. United States Secret Service. *US Secret Service Budget Overview FY 2019 Congressional Justification*. Department of Homeland Security, May 2017, pp 4. https://www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 19 Oct. 2018.

44. The National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*, 22 July 2004, pp. 364. https://govinfo.library.unt.edu/911/report/911Report.pdf . Accessed 1 Aug. 2019.

45. See 34 U.S. Code §%u202F41303 Uniform Federal Crime Reporting Act of 1988 "All departments and agencies within the Federal government (including the Department of Defense) which routinely investigate complaints of criminal activity, shall report details about crime within their respective jurisdiction to theAttorney General in a uniform manner and on a form prescribed by the Attorney General" https://www.law.cornell.edu/uscode/text/34/41303. Accessed 30 Aug. 2019.

46. Baker, Al. “An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported.” *The New York Times*, The New York Times, 5 Feb. 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 10 Oct. 2018.

47. Europol. *Common Taxonomy for Law Enforcement and CSIRTS.* European Union. https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts Accessed 20 Aug. 2019.