CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

OCTOBER 2019

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #5

Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands

Petra Hielkema and Raymond Kleijmeer

Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands

Petra Hielkema and Raymond Kleijmeer

For your convenience, this document contains hyperlinked source notes indicated by this teal colored text.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the authors' own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

+ CONTENTS

Cybersecurity and the Financial System

Carnegie's working paper series 'Cybersecurity and the Financial System' is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Tim Maurer, Co-director of the Cyber Policy Initiative, at tmaurer@ceip.org.

Papers in this Series:

- "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment"
  Lincoln Kaffenberger, Emanuel Kopp, September 2019

- "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box,"
  Tim Maurer and Kathryn Taylor, July 2019

- "The Cyber Threat Landscape: Confronting Challenges to the Financial System"
  Adrian Nish and Saher Naumaan, March 2019

- "Protecting Financial Institutions Against Cyber Threats: A National Security Issue"
  Erica D. Borghard, September 2018

- "Toward a Global Norm Against Manipulating the Integrity of Financial Data"
  Tim Maurer, Ariel (Eli) Levite, and George Perkovich, March 2017

About the Authors

Petra Hielkema is director of the Payments and Market Infrastructure Division in the central bank of the Netherlands (De Nederlandsche Bank).

Raymond Kleijmeer is senior policy officer at the Payments and Market Infrastructure Division in the central bank of the Netherlands (De Nederlandsche Bank).

The views expressed are those by the authors and do not reflect the official views of De Nederlandsche Bank. The authors would like to thank TIBER program manager Rogier Besemer for his review of this paper.

Introduction

Financial institutions face an evolving threat landscape with a wide range of hostile actors targeting them. Regulators and consumers reasonably expect the institutions to make themselves more secure. The question then emerges as to whether financial institutions are complying with the different standards, rules, and regulations regarding their security.

International standard-setting bodies have recognized the need to raise the bar higher for the resilience of financial institutions. The publication of the Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO) guidance on cyber resilience in June 2016 has been pivotal in emphasizing the need to have an integrated approach for financial market infrastructures, with the institution's board being ultimately responsible and accountable for cyber resilience.[1] Increasingly, authorities and financial institutions alike recognize that, in addition to assessing the overall resilience posture of a financial institution against sophisticated attacks, it will be important to actually test this posture. The CPMI-IOSCO guidance includes a chapter dedicated to testing, containing several examples of activities to that end. Recently, frameworks for testing the resilience posture of institutions in practice have been developed internationally.

In the Netherlands, the strong willingness of financial institutions and authorities to test resilience in practice and share information along the way has been one of the key drivers for the initiation, adoption, and implementation of the Threat Intelligence-Based Ethical Red Teaming (TIBER) framework since February 2016. Participating institutions hire external security providers to perform "red team" tests that resemble efforts by sophisticated threat actors in order to test their resilience.[2] The key objective is to enable the financial institutions to learn and evolve based on the test outcomes. In Europe, national central banks and the European Central Bank (ECB) recognized the need to adopt a consistent approach with the publication of the TIBER-EU framework in May 2018.[3]

There is a widespread need for insights on the key issues and decisions about frameworks for testing resilience and about red team testing. This paper reviews and explains the key issues and key decisions taken when initiating, adopting, and implementing the TIBER framework in the Netherlands, where tests of critical financial infrastructures have taken place since 2016.[4] The paper focuses on the more practical aspects of the framework and the first rounds of tests, as well as on the way the work has been embedded in the central bank of the Netherlands (De Nederlandsche Bank—DNB).[5] The paper explains the TIBER framework, its initiation, its preparation, its launch, its testing, and its continuation and extension. It concludes by looking at further international developments and reflecting on some of the key issues in an international context. Thus, the paper presents key lessons learned while developing and implementing the TIBER framework. This paper is intended for a wide international target audience of both authorities of developed and emerging markets and the financial industry in these jurisdictions. It explains the practical implementation aspects of the TIBER framework and key lessons learned from the early experiences in the Netherlands.

The Initiation

Three main forces drove the initiation of the TIBER framework in the Netherlands.

First, financial institutions in the Netherlands have a long history of dealing with threats centering on the customer side of their business. In addition to their customers, products, and channels, sophisticated attacks have targeted the institutions directly in recent years. This necessitates testing approaches that would go beyond what has traditionally been practiced with risk management.

Second, through its role in the international CPMI-IOSCO Working Group on Cyber Resilience, DNB learned about evolving good practices on cyber resilience, including initiatives to strengthen the approach on resilience testing, such as the CBEST framework in the United Kingdom (UK). DNB liaised closely with the Bank of England early to learn from its experiences in that context and used this to develop the TIBER framework. In 2018, with the ECB playing the leading role, a common approach at the European level has evolved. The TIBER-EU framework and CBEST-UK framework resemble each other to a large extent when it comes to the actual testing. One key difference is in the level of engagement by the financial industry in the framework: in the UK, the CBEST program was driven from the supervisory role by the UK authorities with the objective to have institutions comply to the program, whereas in the Netherlands the TIBER program was driven by the central bank playing the role of a convener rather than supervisor—this has fostered a closer level of engagement by the financial industry with the objective to make it a learning experience from the testing (this will be explained in greater detail later).[6]

Third, DNB has acted as a catalyst with regard to security issues within the Dutch financial sector for a long time and established effective working relationships with the financial critical infrastructure. For example, DNB maintains a sector-wide crisis-management structure with established relationships with each of these institutions. Through these contacts, the central bank learned that, although the institutions considered themselves considerably cyber-resilient and invested significantly in their capabilities to protect, detect, and respond to a range of threats, they increasingly realized that being part of an interconnected industry made them at least partially dependent for their own cyber resilience on others in the ecosystem. There were increased calls from the industry to coordinate efforts, to collaborate on the practical aspects of cyber resilience, and to learn from each other's experiences. These relationships formed a basis for trust within the TIBER framework in the Netherlands.

The approach DNB has taken to strengthening cyber resilience consists of building up security fundamentals, strengthening resilience, and the testing framework (see box 1).

Box 1
Fundamentals, Resilience, and Testing

1. Test in practice: It is important to test resilience in practice with sophisticated red team testing to resemble sophisticated threat actors. The benefits of a resilience-testing framework include a more consistent approach in the testing process and clarity on expected quality levels to be achieved by all involved.

2. Strengthen resilience: In the financial system, the bar has been raised in recent years for cyber resilience. Publications include the CPMI-IOSCO guidance on Cyber Resilience for Financial Market Infrastructures in June 2016, building on the Principles for Financial Market Infrastructures of April 2012.

3. Build and maintain security fundamentals: There exist standards and practices implemented for security and operational risk management. Examples include ISO standards for information security, the COBIT Framework and the NIST Cybersecurity framework.

Preparation—How to Get Organized?

Scope of the Framework

When preparing for the establishment of the TIBER framework, a key question was which institutions to involve in developing it as well as undertaking the TIBER test. A useful starting point was the existing designation of several financial institutions as financial critical infrastructure (FCI) based on the nature of their business.[7] Some of the financial institutions that were encouraging the start of a resilience-testing program at DNB were designated as FCIs, as was DNB itself. In short, this group of FCI institutions was well suited to engage with the framework. Some had already built up experience hiring external red team providers, and some had occupied internal red teams; others were relatively new to the game. But all were part of an ecosystem of interdependence for operational continuity.

Obligatory or Voluntary Participation

An important question was whether to make participation in the testing framework obligatory or voluntary. There was a strong preference to start on a voluntary basis for two reasons. First, this would clearly send the message that trust in each institution participating in the framework was high. This reinforced the key assumption and objective of the framework: financial stability is achieved by institutions' capability to learn and evolve in the ever-changing threat landscape. To enhance this capability, the testing would have to be positioned as an exercise that would allow participants to learn and evolve both as individual institutions and as a group. Second, as each participant was a designated FCI, they knew each other as well as their responsibilities toward each other as part of the tripartite crisis management body.

Central Bank and Supervisory Role

Another question that came up frequently was the interaction between the TIBER exercise on the one hand and the supervisory role of DNB on the other. Concerns were raised that in order for a TIBER test to be a successful learning exercise, there could be findings that would result in immediate supervisory measures, which could impact the willingness of participants to really do a daring TIBER test. The following details how these concerns were addressed.

In February 2016, the Financial Stability Committee—consisting of the boards of directors of the Netherlands Authority for the Financial Markets (AFM) and DNB and a high-level representative of the Ministry of Finance—decided to start the TIBER program in February 2016 and develop the framework and perform tests from 2016 to 2018. DNB would manage it and initiate a TIBER framework for resilience testing within the FCIs in close cooperation with industry participants. The TIBER team was positioned on the central bank side of DNB as this would facilitate the many contacts with the financial institutions during the testing in a confidential way. This implied that neither AFM nor DNB would be directly involved in a supervisory role in either the establishment of the TIBER framework or in the testing. Each participating financial institution would inform the supervisor of the test outcomes, provide the supervisor with a summarizing report, and allow for access to more detailed results at the premises of the financial institution. The supervisor would look at the summary of the test outcomes as well as at the remediation plan. The goal was to establish a framework in which the participating financial institutions would hire external security providers that would perform red team tests in accordance with the TIBER guidance to simulate sophisticated cyber attacks on these institutions. The next steps would involve jointly working out the framework guidance together with the industry participants and getting started with the actual testing.

The Launch and Beyond

Private-Public Partnership

The TIBER framework has been a private-public partnership from its launch, with the financial industry supporting its adoption. DNB leveraged its role as an honest broker vis-à-vis participating financial institutions working with each other on a strong basis of trust. The DNB facilitates the sharing of information as well as the different contacts with industry and government agencies involved in the framework. The fact that the DNB has acted primarily as a facilitator for the framework and not as a regulator was designed to add to the trust environment for the framework participants.

Board Involvement

One key issue with the launch of the framework was to involve the boards of the participating financial institutions. As the chief information security officers (CISOs) of the institutions recognized the value added of organizing red team tests in the context of the framework and learning from each other's experiences as well, they showed a strong willingness to participate in the framework. The CISOs explained to their boards the framework's key aspects, and this helped align the institutions' leadership and security management. Had DNB needed to start from the ground up, a first meeting with the responsible board members of the financial institutions likely would have been used just to kick-start the framework. However, as the institutions' security leadership already had paved much of the way in terms of obtaining board-level support for the objective of the framework, the first meeting that took place in June 2016 focused on how to implement the framework.

Parallel Development and Testing

One key question was whether the testing needed to wait until work on developing the TIBER framework was finished. Some of the leading institutions that had already built up experience with red team testing were willing to start the testing in a pilot exercise and incorporate the insights and experiences into the TIBER framework being drafted. Waiting for the TIBER framework to be developed and formalized before starting the testing could have taken considerable time, with the risk of losing momentum for the program to take off. This willingness to start testing and use the lessons learned to improve the framework even before it was published contributed greatly to the framework and helped to show the other financial institutions how to go through the testing process. DNB was part of the group that participated in the pilot in order to demonstrate its commitment to the framework and to experience what it takes to go through a TIBER test.

Program and Test Management Resources

Another key question was whether the participants were willing to devote enough capacity to writing the framework guidance. DNB hired a program manager with industry experience who would be responsible for the TIBER cyber sector team (the TIBER team). DNB also hired a test manager with experience working at a financial institution. This brought first-hand industry know-how to DNB and demonstrated willingness to work together with the private sector to drive the framework forward. The program manager was positioned within DNB, reporting to the director of the Payments and Market Infrastructure Division. A steering group was established with several financial institutions participating and chaired by DNB. The steering group's decisions set the course for the TIBER framework.

A key decision taken early in the process was that the entity undertaking the TIBER test would procure the intelligence and security provider. Staff from the TIBER team guiding the test would be involved in the procurement process in order ensure the quality of the test, the safety of the process, and consistency with the TIBER framework, as well as to share expertise based on the experience of previous tests. However, the responsibility as well as the decision on the procurement would be with the entity itself. Another key decision was that accreditation would not be required at this stage for providers as that market still had to develop.

The Testing

The pilot round of testing was carried out in 2017 on the basis of the first version of the TIBER framework and provided important insights. Box 2 provides an overview of the different stages and explains the roles of the teams involved.

Pilot Phase: Lessons Learned

The pilot round was organized to resemble a normal test with the TIBER framework and in total span six to nine months for each of the tests. The tests provided valuable input for the framework itself. For example, it led to the decision to organize the upfront generic threat intelligence more centrally at the framework level, such as by the TIBER team, rather than having it performed as a first step in each and every test by individual intelligence providers. This reduced the costs for individual institutions and increased consistency for the security providers in how they would resemble threat actors in their testing.

Scenario X

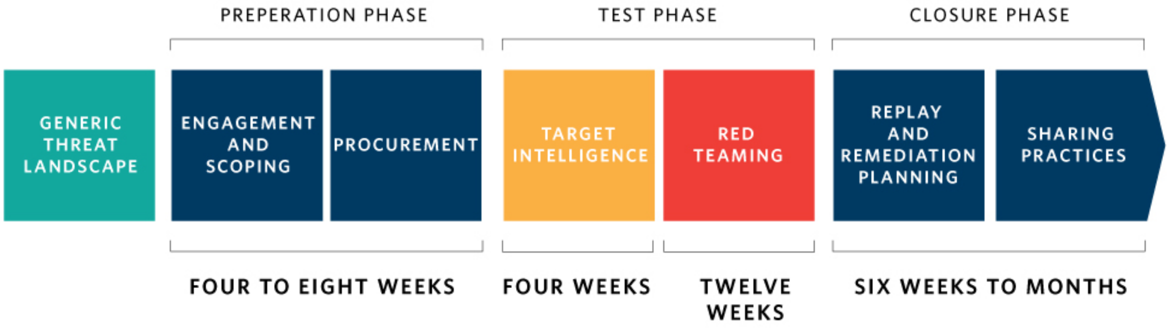
It was decided to add a Scenario X to the TIBER framework, meaning that the test should include a scenario in which the red team would be allowed greater freedom to develop and perform the test based on, for example, tactics, techniques, and procedures that have not yet been seen but are expected in the future.[8] Scenario X is forward-looking and will be used when the testing has advanced to the red team phase, making use of the information gained during the testing. The security providers working on the test can thus perform a more self-developed scenario that could be plausible for the financial institution. This would further enable the institution to prepare its resilience posture to counter current and future threats.

Sufficient Time for Testing

The test phase takes twelve weeks, which covers the different stages of an attack cycle of reconnaissance, getting through the institution's defenses, and exfiltration. It was decided that any TIBER test should include sufficient time to test the later stages of getting through defenses and exfiltration. From a test-management point of view, there are possibilities after having spent a certain amount of time and effort at one stage of testing activities to give a leg up to move to the next stage. This could be useful, for example, in a case where the red team has observed and tested a hardened institution with strong perimeter defenses where it might take considerable time to search for and establish a foothold, leaving little time to test other stages of a typical attack cycle. For this reason, it was decided to include the possibility to advance testing activities to a position deeper inside the institution to continue the test from that point onward. The benefit of this approach is that the institution will be able to test its detection and response capabilities also in these situations. This thus provides a further overall view of its defenses for several phases of an attack.[9]

Box 2

FIGURE 1
The TIBER Framework Test Process and the Roles Involved



Teams Involved

White Team

The white team is the team—within the entity being tested—that is responsible for the overall planning and management of the test, in accordance with the TIBER-EU framework.[10] In the initial stage, the institution's staff involved in the test form a white team, typically consisting of the chief information security officer, an expert, and a board member. Due to the confidential nature of the testing, it is kept as small as possible and is mandated by the board. The white team liaises with the TIBER sector management team on the planning and scoping of the test.[11] Throughout the whole process, the white team maintains close communication as well with the providers that will perform the test. The institution is responsible for the risk management of the testing, as well as for the procurement of a target intelligence and red team provider. The TIBER-EU services procurement guide and white team lead guide helps white teams ensure the quality of the test, the safety of the process, and consistency with the TIBER framework.

Threat Intelligence

The test is divided into two crucial and functionally separate steps. The first is to develop targeted intelligence that will be applied in the red teaming. The threat intelligence is developed by a different team from the one that will perform the red team test. These two teams can be within the same company or can be from two different providers; however, threat intelligence and red teaming are separated. This addresses potential biases in the scenarios used as a red team could intentionally or unintentionally have a bias to certain approaches, for example, based on previous testing experience. This separation thus contributes to the quality of the testing and learning experience.

Red Team

The red team testing must be performed by an external actor. An important factor that contributes to the quality and realism of the red teaming is that the TIBER testing comprises integrated tests that include physical, human, business, and digital aspects designed to closely resemble sophisticated actors in the different scenarios. To further replicate the methods of sophisticated actors, the red team testing covers an extensive period that allows the testers to perform their actions on objectives in a stealthy manner.

Blue Team

The blue team in the TIBER-EU framework consists of the people in the entity that is the subject of the test and whose prevention, detection, and response capabilities are being tested without their foreknowledge. All the parts of the financial institution will be viewed as an attack surface during the test, and this means the whole organization is being tested for its resilience posture and therefore is expected to act as the blue team in defending against the simulated attacks. An important element of the blue team is performed by the cyber defense center in detecting and responding to the different stages of an attack.

It has been observed that after the testing blue teams and red teams find it very helpful to organize a session to replay the test from start to finish and explain the major actions involved at each stage. The institution will additionally follow up the TIBER test with a remediation plan.

TIBER Cyber Sector Team

The TIBER cyber sector team consists of the authority's test manager and at least one other team member acting as backup. This team guides the process of the TIBER test from start to finish. Its roles include maintaining the overall test planning at framework level of the different tests taking place and keeping a close watch on the process and the quality levels performed by the testers. The team also organizes knowledge-sharing meetings for the white team leads and the security providers on a periodic basis to provide feedback loops that will help further improve the capabilities of the different teams involved.

The Continuation and Extension

Sharing Lessons Learned

Since the pilot exercise, all FCI institutions have performed a TIBER test, and these experiences have added value not just for the individual institutions but also for the FCIs as a group, thanks to the information sharing that took place. There are many different kinds of information sharing, from incident reporting to exchanging modus operandi and remedies. The ambition of the TIBER program is to achieve the latter, but the question was how to organize this. The TIBER team decided to organize strictly confidential meetings with small groups of experts, who would decide during the meeting what to share. This turned out to be a successful way to facilitate information sharing. There is a willingness to share lessons learned with others in the same ecosystem if the expertise of the person at the table is at the right level, the person sharing is in control of what is shared and when, and sharing is done in person rather than in writing.

Extension of the Program for 2019–2021

As the TIBER program was scheduled to run until 2018, the Financial Stability Committee as well as DNB had to decide how they wanted to continue. The committee decided to continue the TIBER program for the 2019–2021 period and have all FCIs perform a second TIBER test. It also decided to extend the TIBER framework to several larger institutions in the insurance and pensions industries that, based on their size and function, could exhibit a degree of systemic risk. As the structure and business of these institutions are somewhat different from those of the FCIs, the learning potential of the TIBER program as a whole is likely to be increased by testing these institutions as well. A pilot test with one institution in the insurance industry confirmed the expectations that the TIBER framework could benefit the larger institutions in the insurance and pensions industries.

Finally, at the national level, the government has shown an increased interest in adopting the TIBER approach and initiating resilience testing for other critical infrastructures, including in energy and telecommunications.[12] As the financial system is dependent on those sectors, the widespread adoption of testing in these critical infrastructures is a good step toward more resilience.

International Developments

In Europe, national central banks and the ECB recognized the need to adopt a consistent approach and worked together to develop the TIBER-EU framework, which is now also the leading document for the Netherlands for performing a TIBER test.[13] TIBER-EU was launched in May 2018, and the ECB published its guidelines for the procurement of red team testing services in August 2018 and the white team lead guide in December 2018.[14] These publications contribute in important ways to a consistent approach on red teaming with the TIBER-EU methodology. The ECB has established a knowledge center to foster knowledge sharing on the implementation and adoption of the framework within the Eurosystem.

The added value of resilience testing is becoming increasingly recognized in the financial sector, and there has been interest and adoption of the TIBER methodology in other regions throughout the world. It is good for the financial system as a whole when resilience testing spreads and is performed with a more consistent methodology. At a time when testing resilience is becoming a valued part of risk management, it will be key to avoid multiple frameworks and requirements and to work toward more consistent international approaches. We hope that sharing our experience and lessons learned from establishing the TIBER framework in the Netherlands contributes to the wider adoption and implementation of resilience testing.

Concluding Remarks

One of the key objectives that has been the most challenging yet potentially most rewarding when DNB started the initial plans for the framework was whether it would be possible to create an environment of trust that allowed each to learn from the experiences. This was considered an important key factor for the success of the framework as a whole. And, indeed, this trust in each other has paid off in terms of learning experiences, at the individual level of the testing and especially at the collective level learning from each involved. It has also paid off in continued support by the financial institutions as displayed by their willingness to invest money, time, and effort in the framework. This very much reflects the joint commitment by all involved and provides inspiration for the future course of the TIBER framework.

There has been growing interest abroad in the evolving practices of the TIBER framework, and the insights in this paper can contribute to a more consistent implementation of frameworks internationally. Issues that would require close attention in the implementation and further developments of a framework would include cross-border testing, the expected quality levels of security providers, and how to include third-party providers consistently in the scope of tests. Other industries have also expressed an interest in adopting a framework approach on resilience testing, and there could be more cross-sector testing in the future as well, which would help strengthen collective resilience further. On the principle that a chain is as strong as its weakest link, a wider and consistent adoption of a framework approach on resilience testing would be a very welcome development.

Notes

[1] Committee on Payments and Market Infrastructures-Board of the International Organization of Securities Commissions, “Guidance on Cyber Resilience for Financial Market Infrastructures,” June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[2] The Financial Stability Board’s Cyber Lexicon (from November 2018) defines a red team exercise as a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity’s people, processes, and technology, with minimal foreknowledge and impact on operations. See Financial Stability Board, “Cyber Lexicon,” November 12 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

[3] When the ECB published the TIBER-EU framework, DNB changed the name of its TIBER framework to TIBER-NL. Both frameworks are very much alike. In this paper, the term TIBER refers to the Dutch framework, as the experiences described are based on the period 2016–2018. The term “TIBER-EU” is used when referring to the framework adopted at the EU level. See European Central Bank, “TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming,” May 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

[4] It is beyond the scope of the paper to give a full overview of everything and everyone involved at each stage, although contributions by many have been key to the successful implementation and adoption of the TIBER framework. We express our recognition to all for the efforts that have been crucial to bring the framework to where it now stands.

[5] Additional work is in progress to explain in more detail the key success factors of the red team testing in the TIBER framework. These will be published in a forthcoming DNB working paper. Work is also in progress in cooperation with the Bank for International Settlements’ Financial Stability Institute to explain key issues about the adoption and implementation of resilience-testing frameworks in the larger international financial community, and these will be published in a forthcoming FSI Insights.

[6] Another difference is that security industries in the UK and in the Netherlands and the wider EU showed different characteristics, with in the UK the industry body CREST playing a role to certify security providers for the CBEST framework. For TIBER-EU, the ECB published security provider guidelines in August 2018.

[7] This structure had been established by the tripartite crisis management body consisting of the boards of directors of the Authority Financial Markets (AFM), DNB, and a high-level representative of the Ministry of Finance. The committee becomes operational in the event of an actual or imminent major disruption of the payment or securities systems.

[8] Derived from ECB’s TIBER-EU guide, May 2018.

[9] For a more detailed description of the different stages, see the TIBER-EU framework guide published in May 2018.

[10] Definition derived from European Central Bank, “TIBER-EU White Team Guidance: The Roles and Responsibilities of the White Team in a Threat Intelligence-Based Ethical Red Teaming Test,” December 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf.

[11] The guiding role of the TIBER sector management team is required from the first stage to the final stage for a test to qualify as a TIBER test.

[12] During the international cybersecurity One Conference (October 1–3, 2018), the Netherlands’ minister of justice and security announced that one of the first three project of the Dutch Cybersecurity Alliance would be to extend the TIBER-NL framework to other critical sectors in the country.

[13] With the publication of the TIBER-EU framework in May 2018, this is now the document used for guidance of a TIBER-NL test and as such has rendered obsolete the earlier published version of the TIBER-NL guide of November 2017.

[14] European Central Bank, "TIBER-EU Framework: Services Procurement Guide," August 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf?d8287db19b73ac0cb6412d8fa0fb08c2; and ECB, "TIBER-EU White Team Guidance."

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org