Steven Maijoor: State of the ART - DNB launches a new cyber security test framework

Speech by Mr Steven Maijoor, Executive Director of Supervision of the Netherlands Bank, at the Advanced red teaming (ART) launch event, Amsterdam, 10 April 2024.

* * *

Hello everyone, and welcome.

Today, we have good reason to celebrate. Because we are launching a brand new framework to test our society's resilience against cyberattacks. We're launching: ART – which stands for 'Advanced Red Teaming'.

Usually, when you have something to celebrate, there's cake. Maybe even candles. And definitely a card with some nice words.

Today, there's none of that – but we do have bitterballen.

And, we have you – CISOs from the financial sector, the healthcare sector, the telecom sector and our government.

And we have my colleagues from De Nederlandsche Bank who put their hearts and souls into developing ART.

And if we combine this, we've got something far better than candles, cards or cake. We've got a cause. A cause to protect our society against cyber threats, cyberattacks and cyber criminals.

Unfortunately, that is necessary. You know this. And we know this. All of us here, today, know that all over the world, across all different sectors, cyberattacks have become a standard instrument in both criminal and military toolkits. Or, for that matter, in any type of threat-actor's toolkit, regardless of their motivation.

The ongoing war in Ukraine, for instance, will not only be won in the trenches, with boots on the ground, regaining terrain, step by step. It will also need to be fought online, with hands on the keyboard, defending liberty – bit by bit, byte by byte.

Like we witnessed recently – when the Ukrainian telecom provider Kyivstar was attacked. Not by bombs. Not by missiles. But through cyberspace. This attack hit a vital infrastructure of Ukrainian society – and left 24 million people struggling to communicate.

The attack also caused significant second tier damage. Because the attack on Kyivstar also hit ATMs that used the company's SIM cards. Leaving people struggling to get cash.

Closer to home, our military intelligence warned about Chinese hackers trying to infiltrate critical Dutch infrastructure, planting threats that would lay dormant till activated – and then cause havoc from half a world away.

Like I said, all of us are aware of these threats.

In fact, a part of DNB's cyber strategy is monitoring and reporting on the cyber threats for the financial sector. Even more, we also organise and coordinate cyber crisis and red teaming exercises.

But the fact remains as simple as uncomfortable: cyber threats will not go away. And the increasing scale and scope of cyber threats are not news to you. Neither are the costs and calamities that result from actual attacks.

But what is new, is the framework we are launching today: ART. Because one fact, as simple as it is comforting, is that you and I share a common cause – we will not stop fighting cyber threats.

So, let me tell you a bit more about what ART is and why we built it.

With ART, you voluntarily sign up to get your core IT infrastructure hacked – not to steal your assets, but to seal your weak spots.

Doing an ART test means that a real cyberattack is simulated as closely as possible. To do so, the attack plays out a plausible, threat-intelligence based scenario. So, it is based on the actual capabilities and motivations of existing malicious actors – be they state or non-state, geopolitical or criminal.

During the test, only a handful of people – from both within and outside your organisation – know about the actual attack.

As such, ART helps to identify your weak spots – it helps you to see how much damage a malicious actor could cause, how long it takes you to discover the foul play, and how much time you need to get back on your feet and mitigate the damage.

I can hear many of you think: don't we already have such a framework?

Yes, indeed – ART builds on our earlier, successful framework, TIBER, which stands for Threat-Intelligence Based Ethical Red-teaming. TIBER is an ethical hacking framework, developed in 2016, to test the cyber security of our core financial infrastructure, such as large banks and payment institutions. With TIBER, an institution's people, processes and pivotal IT infrastructure could be targeted.

The development of ART benefited tremendously from eight years of TIBER experience – both in terms of quality standards as in successful deployment.

So, with ART, we definitely don't have to start from scratch – in a sense, we can stand on the shoulders of a giant. Which, I think, is fair to say, especially since TIBER has been embraced by 17 central banks all over Europe. And even by the European co-legislators, given that starting January 2025, TIBER will be included in European law and will then be called TLPT: Threat-Led Penetration Testing.

Still, there was a clear need for something more, something alongside TIBER or TLPT. A need that could be summarised as a need for a voluntary test framework, one that is more modular, so that it can be tailored more easily to the specific testing needs of an organisation. Of your organisation. And ART is our answer to this need – ready for you to use.

Whether you are a small or a large organisation – the former is no less important, sometimes the opposite is in fact the case.

Whether you have an advanced cyber security policy, or one that is more limited in terms of scale and scope.

Or whether you operate in the financial sector, or elsewhere – like the healthcare or the telecom sector, or the government.

Later today, you will get a more detailed presentation on ART. This will give you the opportunity to ask all your questions – about ART, TIBER or TLPT. But really – with this new framework, with ART, there is no reason not to test your cyber security. Whether it is a very specific real-life scenario you want to test, or whether you want to use it as a stepping stone to TIBER, or even to set it up as a test that goes beyond TIBER. The modular set-up of ART will make testing more accessible and hence increase our overall cyber resilience.

And that is necessary.

It is an unpleasant realisation, but actual lives are at stake in what is essentially a numbers game. A game of ones and zeros. A game of investing time and money into protecting those ones and zeros, and hence yourself and the people who rely on you – whether it's for your financial expertise, your medical care, your communication infrastructure or as their political representatives.

You and I know that testing your cyber security and subsequently improving it – if and where needed – is an effective way to keep hackers out. You and I know, that it takes time and money to do so. But we also all know that your time and money are not unlimited.

That is why we are launching ART. A new framework we strongly believe in. A voluntary, modular framework that was built in response to the needs of the financial sector and beyond; one that has proven its value in pilot tests; and one that, in the meantime, has received encouraging reactions from the ECB.

I therefore want to call upon everyone here today to start using ART – in whatever form suits you. To start using this state of the art framework to learn about the state of your cybersecurity, and hence, to take an improved stance in our joint fight against cyber threats.

And don't shy away from spreading the word – the ART we are talking about today, is not one for the few, it is one for the many.

Dear CISOs, it is heart-warming to see so many of you here, today – from the financial sector, the healthcare sector, the telecom sector, and the Dutch government. Each one of you plays a vital role in our society – a role that becomes even more vital, the more connected we become, whether you share software, service providers, or cyber risks.

Maybe we'll reconvene in the future, and then there will be cake. And candles. And cards. And hopefully we will be celebrating the success of ART, the success of a common cause: our fight against cyberthreats.

We're not there yet, but I am confident we will get there – stronger and more resilient than ever.

Together, we'll protect our organisations, our people and our society.

And today marks another step forward. And that alone is very much reason to celebrate. So let's celebrate!

Thank you.