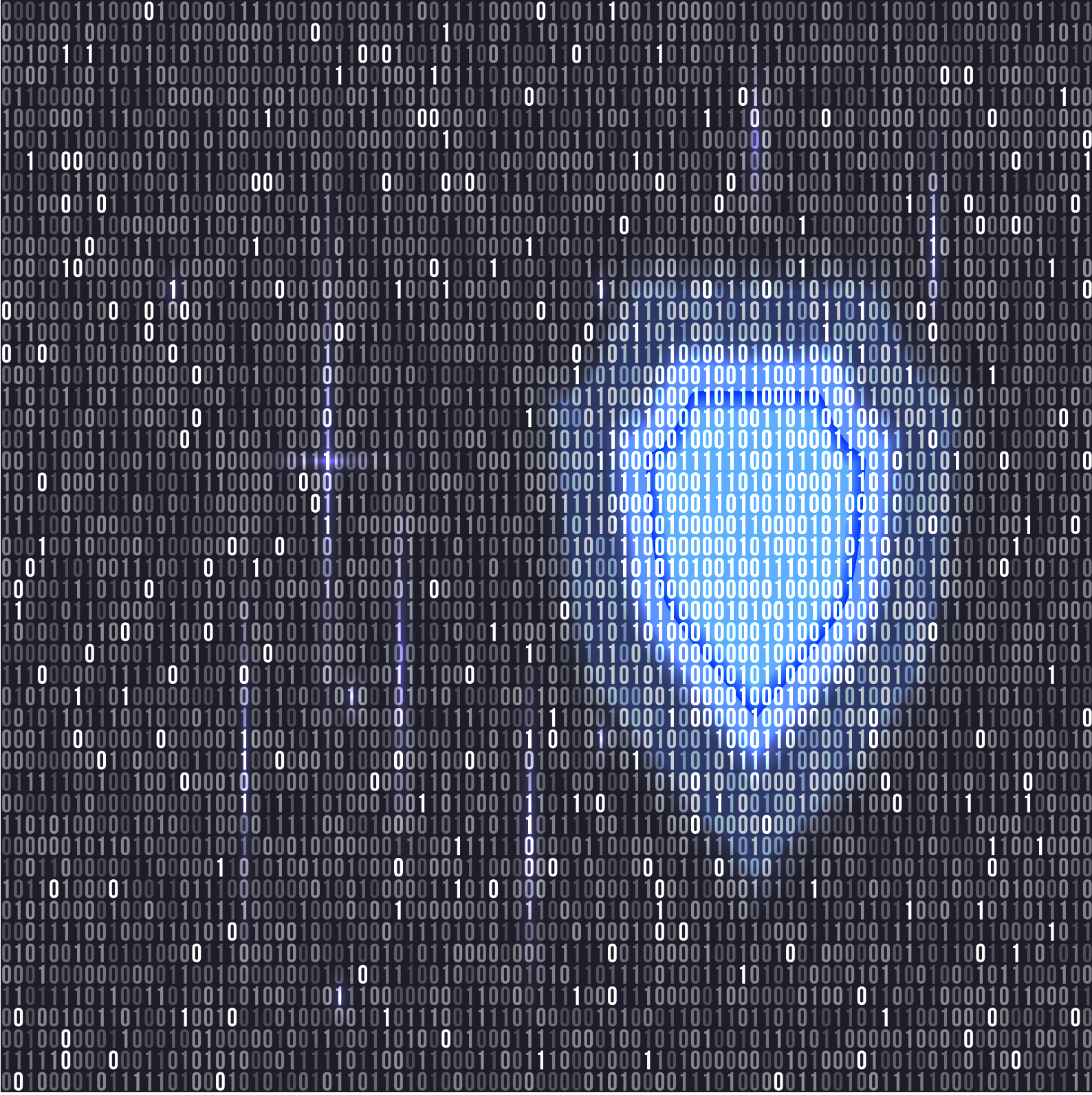

HCSEC 2019 ANNUAL REPORT

Why this UK report matters to Ireland.

RIVADA NETWORKS

www.rivada.com

HCSEC 2019 ANNUAL REPORT

Why this UK report matters to Ireland.

What is the HCSEC?

The HCSEC was established by Huawei at the UK Government's request eight years ago to evaluate Huawei technology for security vulnerabilities before deployment into UK telecoms networks. It has been engaged in testing for five years. The HCSEC is funded by Huawei but staffed by British staff, including people formerly employed by GCHQ.

The work of HCSEC is overseen by an Oversight Board co-chaired by the UK's NCSC and Huawei.

The March 2019 Annual Report highlights that Huawei has made little progress. While it has promised to rectify vulnerabilities and their global software engineering and cyber security processes, Huawei has delivered very little. The report clearly states that no guarantee could be given that Huawei did not present a cyber security risk.

What does it investigate?

The HCSEC investigates the following aspects of Huawei technology:

- Engineering processes and practices;
- Source code quality for software and hardware, including third-party.

The HCSEC works with Huawei to monitor progress to rectify any shortcomings or issues with Huawei software, hardware or processes identified by the Lab.

The HCSEC publishes a high-level public report each year into the progress made by Huawei to rectify these shortcomings and offers a reassurance level on the risk of Huawei technology in the UK telecoms ecosystem.

It is important to note that any of the risks identified by the HCSEC are not risks limited to the UK. These are global risks associated with Huawei technology.

Implications for Ireland

The HCSEC report should be of particular interest to Ireland as a number of Irish Mobile Operators have confirmed their intention of deploying either upgrades or 5G networks utilising Huawei technology - most notably Eir and Three Mobile. Both operators intend to start this deployment in 2019.

Irish mobile operators have enjoyed relatively light regulation compared to many other countries. The EU Directive on security of network an information systems (NIS Directive), adopted in 2016, saw mobile operators in Ireland designated as Operators of Essential Services (OES). Such OES are required to comply with state-led cyber security requirements to ensure the safety and operation of Irish critical infrastructure.

Electricity network operators are also designated as OES. We understand that at least one Electricity OES is using Huawei technology in the management of their infrastructure. This report has implications for this also.

This report may indicate that Irish mobile networks are as susceptible to attack as those in the UK utilising Huawei equipment and software. Ireland is highly dependent on mobile networks for communication and any interruption to mobile networks would have a large impact economically, socially and for state security.

It has been extremely difficult to ascertain a transparent chain-of-command for cyber security in Ireland as Ireland operates a cross-departmental and cross-agency competency for various aspects of state cyber-security. The HCSEC report should be of particular interest to the Irish NCSC.

For the purposes of interested stakeholders Rivada Networks is providing a summary of the key points raised by the HCSEC 2019 Annual Report.

Key Issues

HCSEC has previously highlighted a number of risks that it wanted Huawei to resolve. Huawei failed to do so, and the HCSEC has now identified many more risks, compounding the issue of binary equivalence, and sloppy coding. It is apparent that these are global risks rather than risks specific to the UK market.

New additional risks are 'significant'

The report does not explain what these are, but clearly states these risks are 'significant'. The risks revolved around Huawei engineering processes - the genesis of coding and manufacturing - which is an alarm bell sounding on Huawei supply chain security.

Huawei has not fixed previously identified vulnerabilities

Despite promising £2bn to fix those issues identified in the previous report, and to do so in two-to-five years, the HCSEC has not been able to identify significant progress in rectifying these vulnerabilities. Huawei is promising much, but delivering very little.

Risk-managing future Huawei tech 'difficult'

Given the issues of binary equivalency, different engineering processes and sloppy coding the HCSEC cannot give assurances that it will be able to effectively risk-manage any new technology Huawei develops for cellular networks. This is a serious risk for 5G and Smart Places / IOT technologies.

Little confidence that Huawei can meet its commitment to fix vulnerabilities

The report indicates that the HCSEC has little to no confidence that Huawei can fix its security vulnerabilities. What plans Huawei has presented to the HCSEC to remedy engineering and security vulnerabilities have been deemed INADEQUATE.

Huawei uses archaic engineering processes

The report clearly states that Huawei does not use modern 'agile' software engineering process and that the HCSEC has little confidence in the processes Huawei does use. Furthermore, the report states that those modern configuration management processes that Huawei does use are not universally applied throughout Huawei, leading to confusing methodologies.

A Huawei-powered network could be critically damaged

The report highlights that there is no end-to-end integrity in multiple processes and configurations. If a Huawei-powered network were attacked Huawei might not be able to identify the issue and the network might be critically damaged.

Huawei Operating System vulnerable

Huawei uses an outdated and not widely utilized operating system that has a number of major security risks attached to it, and would incur severe outage if it were impacted. The report states that **the NCSC does not believe that Huawei has any credible, secure plan to reduce the cyber security risk associated with the use of this 3rd party operating systems.** It further states that the Huawei alternative operating system is subject to the same weak software engineering processes and binary equivalency issues and therefore **cannot be deemed to be a secure, viable alternative.**

Huawei's entire software life-cycle management system flawed

The report clearly states that the Huawei software life-cycle management system **is flawed, and full of major security vulnerabilities.** The Huawei solution offered was still inadequate, with serious security issues.

No confidence in Huawei's ability to solve cyber security issues

The NCSC and HCSEC have **little to no confidence** in Huawei's ability to remediate the software engineering and cyber security issues in the LTE eNodeB product development and sustained engineering cycle.

Huawei equipment had hundreds of vulnerabilities in 2018

Several hundred Huawei vulnerabilities had to be reported to UK operators in 2018 alone. **Not all of these vulnerabilities have been resolved and are still in active networks in the UK.**

Key takeaways

- The HCSEC cannot provide an assurance that Huawei is not a cyber security risk;
- Despite apparently cooperating, Huawei are not meeting milestones agreed to resolve security issues;
- Managing future Huawei risk is going to be very difficult;
- Huawei networks are vulnerable now, 5G Huawei networks will be more vulnerable;
- If a hostile actor or state has knowledge of Huawei vulnerabilities they could cause major network disruption.

Rivada Recommends

- Huawei represents an unacceptable risk to critical infrastructure and utilities and should be precluded from 5G network deployment;
- Huawei also represents an unacceptable risk to power and water critical infrastructure and should be precluded from providing solutions in these areas;
- Any OES that currently utilises or plans to utilise Huawei equipment should begin a review of these contracts in order to cancel said projects: the Irish Government should provide the necessary framework to assist OES in this regard.

Rivada Networks shall make a comprehensive submission to the Dept. of Communications, Climate Action & Environment with a list of over 20 key recommendations for the National Cyber Security Strategy to ensure vendors that present a security risk to Irish critical infrastructure are precluded from the Irish critical infrastructure IOT ecosystem.

Rivada Networks is a leading designer and integrator of fixed infrastructure and mobile communication systems and networks. Rivada has been engaged to modernise networks in over 30 U.S. states and has been the prime contractor in the design, installation and implantation of new networks to meet the stringent cyber security standards set by U.S. Federal agencies. We work directly with the leading network security specialists to deliver modern, comprehensive, secure, interoperable communication systems.

Rivada recognises that with the advent of 5G and the creation of new technologies such as smart cities and smart utilities it is vital that ireland's cyber security be as robust and as futurist as possible; recognising the pace of the technological evolution in mobile communications.

Authors:
Dr. Steve Conlon, VP Corporate Intelligence, Rivada Networks
Mr. John McGuirk, VP Corporate Communications, Rivada Networks

This material has been prepared for general informational purposes only.

www.rivada.com